Kết quả phân tích

# Không rõ tiêu đề QUY CHẾ AN TOÀN THÔNG TIN Mã số: QC.IT.001 Lần ban hành: 01 Tài liệu này chứa các thông tin là tài sản của NCB. Cấm sao chép, in ấn dưới mọi hình thức nếu không được sự cho phép của NCB. 7/48 NCB - Tài liệu nội bộ STT Tên văn bản Số hiệu văn bản Nơi ban hành Ngày ban hành Internet (Sửa đổi, bổ sung 35/2016/TT-NHNN) 6 Quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng 09/2020/TT- NHNN NHNN 21/10/2020 7 Triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng 2345/QĐ- NHNN NHNN 18/12/2023

## 2.2 Văn bản định chế của NCB STT Tên văn bản Số hiệu văn bản Mã văn bản 1 Điều lệ của Ngân hàng TMCP Quốc Dân 2 Quy định về quản lý rủi ro hoạt động với hoạt động thuê ngoài QĐ.RR.024

**AI trả lời:** Dựa trên thông tin được cung cấp, đánh giá về quy chế an toàn thông tin "Không rõ tiêu đề QUY CHẾ AN TOÀN THÔNG TIN Mã số: QC.IT.001" như sau:  
  
\*\*Đánh giá:\*\* Cần xem xét thêm.  
  
\*\*Lý do:\*\*  
  
\* \*\*Thiếu thông tin về nội dung quy chế:\*\* Thông tin cung cấp chỉ đề cập đến tên, mã số, tính chất bảo mật của tài liệu và danh mục các văn bản tham chiếu. Không có nội dung cụ thể của quy chế để đánh giá mức độ phù hợp với các yêu cầu tối thiểu được nêu trong Điều 6 của thông tư (Quản lý tài sản CNTT, quản lý nguồn nhân lực, bảo đảm an toàn vật lý và môi trường).  
\* \*\*Tham chiếu đến các văn bản pháp luật:\*\* Quy chế có tham chiếu đến Thông tư 09/2020/TT-NHNN về an toàn hệ thống thông tin trong hoạt động ngân hàng, cho thấy có sự quan tâm đến việc tuân thủ các quy định của pháp luật. Tuy nhiên, cần xem xét nội dung cụ thể của quy chế để đánh giá mức độ tuân thủ thực tế.  
\* \*\*Tính chất nội bộ:\*\* Quy chế được xác định là "Tài liệu nội bộ" của NCB, điều này phù hợp với yêu cầu tại Khoản 1 Điều 6 về việc tổ chức xây dựng quy chế phù hợp với hệ thống thông tin, cơ cấu tổ chức, yêu cầu quản lý và hoạt động của tổ chức.  
  
\*\*Gợi ý sửa đổi/kiểm tra bổ sung:\*\*  
  
1. \*\*Bổ sung thông tin về nội dung quy chế:\*\* Cần cung cấp nội dung chi tiết của quy chế để đánh giá mức độ phù hợp với các yêu cầu tối thiểu được quy định tại Khoản 2 Điều 6 của thông tư (quản lý tài sản CNTT, quản lý nguồn nhân lực, bảo đảm an toàn về mặt vật lý và môi trường lắp đặt).  
2. \*\*Kiểm tra tính đầy đủ và phù hợp:\*\* Đảm bảo quy chế bao gồm đầy đủ các nội dung cơ bản theo yêu cầu của pháp luật và phù hợp với đặc thù hoạt động của NCB.  
3. \*\*Rà soát tính cập nhật:\*\* Kiểm tra xem các văn bản tham chiếu (đặc biệt là Thông tư 09/2020/TT-NHNN) có còn hiệu lực và quy chế có được cập nhật để phù hợp với các thay đổi của pháp luật hay không.  
4. \*\*Đảm bảo phê duyệt và triển khai:\*\* Xác nhận rằng quy chế đã được người đại diện hợp pháp của NCB ký ban hành và được triển khai thực hiện trong toàn tổ chức theo đúng quy định tại Khoản 1 Điều 6.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 37. Yêu cầu về an toàn, bảo mật các hệ thống thông tin**  
1. Xây dựng tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin. Trong đó các yêu cầu về an toàn, bảo mật được xây dựng đồng thời với việc xây dựng các yêu cầu kỹ thuật, nghiệp vụ.  
  
2. Xây dựng phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu. Kết quả kiểm tra phải lập thành báo cáo và được cấp có thẩm quyền phê duyệt trước khi đưa vào vận hành chính thức.

**Điều 3. Nguyên tắc chung**  
3. Các rủi ro công nghệ thông tin có thể xảy ra trong tổ chức được nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả.  
  
4. Việc xây dựng, triển khai quy chế an toàn thông tin được thực hiện trên cơ sở các quy định tại Thông tư này và hài hòa giữa lợi ích, chi phí và cấp độ chấp nhận rủi ro của tổ chức.

**Điều 24. Trao đổi thông tin**  
3. Các thông tin bí mật phải được mã hóa hoặc áp dụng các biện pháp bảo mật thông tin trước khi trao đổi. Đối với hệ thống thông tin cấp độ 5, tổ chức phải sử dụng kết nối mạng an toàn và các thiết bị, phương tiện chuyên dụng để mã hóa, giải mã thông tin bí mật và khi trao đổi thông tin.  
  
4. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp.

**Điều 6. Quy chế an toàn thông tin**  
Điều 6. 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;

#### Luat\_tin\_dung.docx

**Điều 146. Thẩm quyền quyết định cơ cấu lại tổ chức tín dụng được kiểm soát đặc biệt**  
b) Phê duyệt phương án chuyển giao bắt buộc, phá sản tổ chức tín dụng được kiểm soát đặc biệt;  
  
c) Quyết định áp dụng biện pháp đặc biệt nhằm bảo đảm an toàn hệ thống tổ chức tín dụng, trật tự, an toàn xã hội khi xử lý tổ chức tín dụng được kiểm soát đặc biệt và báo cáo Quốc hội tại kỳ họp gần nhất.  
  
2. Thủ tướng Chính phủ có thẩm quyền sau đây:

## 2.3 Trong văn bản này các văn bản, tài liệu tham chiếu sẽ bao gồm các văn bản sửa đổi, bổ sung của chúng.

**AI trả lời:** Dựa trên thông tin được cung cấp, đánh giá "QUY CHẾ AN TOÀN THÔNG TIN Mã số: QC.IT.001" như sau:  
  
\*\*Đánh giá:\*\* Cần xem xét thêm.  
  
\*\*Lý do:\*\*  
  
\* \*\*Phù hợp:\*\*  
 \* Quy chế an toàn thông tin được xây dựng trên cơ sở các quy định tại Thông tư và hài hòa giữa lợi ích, chi phí và cấp độ chấp nhận rủi ro của tổ chức (điểm 6).  
\* \*\*Cần xem xét thêm:\*\*  
 \* Cần xem xét quy chế này có bao gồm các nội dung sau hay không:  
 \* Xây dựng tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin, trong đó các yêu cầu về an toàn, bảo mật được xây dựng đồng thời với việc xây dựng các yêu cầu kỹ thuật, nghiệp vụ (điểm 1).  
 \* Xây dựng phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu. Kết quả kiểm tra phải lập thành báo cáo và được cấp có thẩm quyền phê duyệt trước khi đưa vào vận hành chính thức (điểm 2).  
 \* Các rủi ro công nghệ thông tin có thể xảy ra trong tổ chức được nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả (điểm 3).  
 \* Thông tin bí mật phải được mã hóa hoặc áp dụng các biện pháp bảo mật thông tin trước khi trao đổi. Đối với hệ thống thông tin cấp độ 5, tổ chức phải sử dụng kết nối mạng an toàn và các thiết bị, phương tiện chuyên dụng để mã hóa, giải mã thông tin bí mật và khi trao đổi thông tin (điểm 3).  
 \* Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp (điểm 4).  
 \* Triển khai các giải pháp an ninh mạng tại các cổng kết nối Internet để bảo đảm an toàn trước các hiểm họa tấn công từ Internet vào mạng nội bộ của tổ chức (điểm 3).  
 \* 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 tổ chức thông qua cổng kết nối Internet (điểm 4).  
 \* Phân quyền đọc, ghi, xóa, thực thi đối với thông tin, dữ liệu, chương trình (điểm b).  
 \* Các hệ thống thông tin sử dụng chung nguồn tài nguyên phải được cấp có thẩm quyền phê duyệt (điểm 4).  
 \* Đối với máy chủ thuộc hệ thống thông tin từ cấp độ 3 trở lên và các hệ thống thông tin có xử lý thông tin cá nhân của khách hàng phải sử dụng giao thức kết nối an toàn và có phương án chống đăng nhập tự động (điểm 5).  
  
\*\*Gợi ý sửa đổi:\*\*  
  
\* Cần rà soát và bổ sung các nội dung còn thiếu để đảm bảo quy chế bao quát đầy đủ các yêu cầu về an toàn thông tin theo quy định.  
\* Cần làm rõ phạm vi áp dụng của quy chế (ví dụ: áp dụng cho hệ thống thông tin cấp độ nào, đối tượng nào).  
\* Cần có quy trình xem xét và cập nhật quy chế định kỳ để đảm bảo tính phù hợp với các thay đổi về công nghệ và quy định pháp luật.  
\* Cần bổ sung các điều khoản về trách nhiệm của các bên liên quan trong việc thực thi quy chế.  
\* Cần có quy trình đánh giá hiệu quả của quy chế.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 24. Trao đổi thông tin**  
3. Các thông tin bí mật phải được mã hóa hoặc áp dụng các biện pháp bảo mật thông tin trước khi trao đổi. Đối với hệ thống thông tin cấp độ 5, tổ chức phải sử dụng kết nối mạng an toàn và các thiết bị, phương tiện chuyên dụng để mã hóa, giải mã thông tin bí mật và khi trao đổi thông tin.  
  
4. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp.

**Điều 37. Yêu cầu về an toàn, bảo mật các hệ thống thông tin**  
1. Xây dựng tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin. Trong đó các yêu cầu về an toàn, bảo mật được xây dựng đồng thời với việc xây dựng các yêu cầu kỹ thuật, nghiệp vụ.  
  
2. Xây dựng phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu. Kết quả kiểm tra phải lập thành báo cáo và được cấp có thẩm quyền phê duyệt trước khi đưa vào vận hành chính thức.

**Điều 3. Nguyên tắc chung**  
3. Các rủi ro công nghệ thông tin có thể xảy ra trong tổ chức được nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả.  
  
4. Việc xây dựng, triển khai quy chế an toàn thông tin được thực hiện trên cơ sở các quy định tại Thông tư này và hài hòa giữa lợi ích, chi phí và cấp độ chấp nhận rủi ro của tổ chức.

**Điều 31. Quản lý kết nối Internet**  
3. Triển khai các giải pháp an ninh mạng tại các cổng kết nối Internet để bảo đảm an toàn trước các hiểm họa tấn công từ Internet vào mạng nội bộ của tổ chức.  
  
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 tổ chức thông qua cổng kết nối Internet.  
  
Mục 6. QUẢN LÝ SỬ DỤNG DỊCH VỤ CÔNG NGHỆ THÔNG TIN CỦA BÊN THỨ BA

**Điều 30. Quản lý truy cập hệ thống thông tin và ứng dụng**  
b) Phân quyền đọc, ghi, xóa, thực thi đối với thông tin, dữ liệu, chương trình.  
  
4. Các hệ thống thông tin sử dụng chung nguồn tài nguyên phải được cấp có thẩm quyền phê duyệt.  
  
5. Đối với máy chủ thuộc hệ thống thông tin từ cấp độ 3 trở lên và các hệ thống thông tin có xử lý thông tin cá nhân của khách hàng phải sử dụng giao thức kết nối an toàn và có phương án chống đăng nhập tự động.

# Điều 3. Giải thích từ ngữ

## 3.1 NCB/ Ngân hàng: Là Ngân hàng Thương mại Cổ phần Quốc Dân;

**AI trả lời:** Không tìm thấy tài liệu liên quan.

### Tài liệu tham khảo:

#### Luat\_ngan\_hang\_nha\_nuoc.docx

**Điều 2. Vị trí và chức năng của Ngân hàng Nhà nước Việt Nam**  
Điều 2. Vị trí và chức năng của Ngân hàng Nhà nước Việt Nam  
1. Ngân hàng Nhà nước Việt Nam (sau đây gọi là Ngân hàng Nhà nước) là cơ quan ngang bộ của Chính phủ, là Ngân hàng trung ương của nước Cộng hoà xã hội chủ nghĩa Việt Nam.  
  
2. Ngân hàng Nhà nước là pháp nhân, có vốn pháp định thuộc sở hữu nhà nước, có trụ sở chính tại Thủ đô Hà Nội.

**Điều 2. Vị trí và chức năng của Ngân hàng Nhà nước Việt Nam**  
2. Ngân hàng Nhà nước là pháp nhân, có vốn pháp định thuộc sở hữu nhà nước, có trụ sở chính tại Thủ đô Hà Nội.  
  
3. Ngân hàng Nhà nước thực hiện chức năng quản lý nhà nước về tiền tệ, hoạt động ngân hàng và ngoại hối (sau đây gọi là tiền tệ và ngân hàng); thực hiện chức năng của Ngân hàng trung ương về phát hành tiền, ngân hàng của các tổ chức tín dụng và cung ứng dịch vụ tiền tệ cho Chính phủ.

**Điều 4. Nhiệm vụ, quyền hạn của Ngân hàng Nhà nước**  
21. Tổ chức thực hiện hợp tác quốc tế về tiền tệ và ngân hàng.  
  
22. Đại diện cho Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam tại các tổ chức tiền tệ và ngân hàng quốc tế.  
  
23. Tổ chức hệ thống thông tin tín dụng và cung ứng dịch vụ thông tin tín dụng; thực hiện chức năng quản lý nhà nước đối với các tổ chức hoạt động thông tin tín dụng.  
  
24. Làm đại lý và thực hiện các dịch vụ ngân hàng cho Kho bạc Nhà nước.

**Điều 4. Nhiệm vụ, quyền hạn của Ngân hàng Nhà nước**  
Điều 4. Nhiệm vụ, quyền hạn của Ngân hàng Nhà nước  
1. Hoạt động của Ngân hàng Nhà nước nhằm ổn định giá trị đồng tiền; bảo đảm an toàn hoạt động ngân hàng và hệ thống các tổ chức tín dụng; bảo đảm sự an toàn, hiệu quả của hệ thống thanh toán quốc gia; góp phần thúc đẩy phát triển kinh tế - xã hội theo định hướng xã hội chủ nghĩa.  
  
2. Tham gia xây dựng chiến lược và kế hoạch phát triển kinh tế - xã hội của đất nước.

**Điều 52. Đối tượng thanh tra ngân hàng**  
2. Tổ chức có hoạt động ngoại hối, hoạt động kinh doanh vàng; tổ chức hoạt động thông tin tín dụng; tổ chức cung ứng dịch vụ trung gian thanh toán không phải là ngân hàng;  
  
3. Cơ quan, tổ chức, cá nhân Việt Nam và cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam trong việc thực hiện các quy định của pháp luật về tiền tệ và ngân hàng thuộc phạm vi quản lý nhà nước của Ngân hàng Nhà nước.

## 3.2 Đơn vị: Là Các Khối/Trung tâm trực thuộc Hội sở NCB và các Chi nhánh/Phòng giao dịch trong Cơ cấu tổ chức của NCB;

**AI trả lời:** Không tìm thấy tài liệu liên quan.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 47. Trung tâm Điều hành an ninh mạng**  
1. Tổ chức quản lý trực tiếp hệ thống thông tin từ cấp độ 3 trở lên phải thành lập hoặc chỉ định bộ phận chuyên trách để quản lý vận hành Trung tâm Điều hành an ninh mạng (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, tổ chức tài chính vi mô, quỹ tín dụng nhân dân cơ sở, công ty thông tin tín dụng, Công ty Quản lý tài sản của các tổ chức tín dụng Việt Nam, Nhà máy in tiền quốc gia).

**Điều 55. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước**  
4. Ngân hàng Nhà nước chi nhánh tỉnh, thành phố có trách nhiệm thanh tra việc thực hiện Thông tư này tại các tổ chức trên địa bàn và xử lý vi phạm hành chính đối với hành vi vi phạm Thông tư này theo quy định của pháp luật.

**Điều 50. Xây dựng hệ thống dự phòng thảm họa**  
2. Các tổ chức chỉ có một trụ sở làm việc tại Việt Nam (trừ tổ chức tài chính vi mô, quỹ tín dụng nhân dân cơ sở) phải có văn phòng dự phòng tại một địa điểm khác tách biệt trụ sở làm việc và có trang thiết bị để bảo đảm hoạt động liên tục thay thế trụ sở làm việc.

**Điều 5. Phân loại hệ thống thông tin**  
c) Hệ thống cơ sở hạ tầng thông tin quốc gia trong ngành Ngân hàng phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế.  
  
7. Trong trường hợp hệ thống thông tin bao gồm nhiều hệ thống thành phần, mỗi hệ thống thành phần lại tương ứng với một cấp độ khác nhau, cấp độ hệ thống thông tin được xác định là cấp độ cao nhất trong các cấp độ của các hệ thống thành phần cấu thành.

#### Luat\_ngan\_hang\_nha\_nuoc.docx

**Điều 4. Nhiệm vụ, quyền hạn của Ngân hàng Nhà nước**  
9. Cấp, sửa đổi, bổ sung, thu hồi giấy phép thành lập và hoạt động của tổ chức tín dụng, giấy phép thành lập chi nhánh ngân hàng nước ngoài, giấy phép thành lập văn phòng đại diện của tổ chức tín dụng nước ngoài, tổ chức nước ngoài khác có hoạt động ngân hàng; cấp, thu hồi giấy phép hoạt động cung ứng dịch vụ trung gian thanh toán cho các tổ chức không phải là ngân hàng; cấp, thu hồi giấy phép hoạt động cung ứng dịch vụ thông tin tín dụng cho các tổ chức; chấp thuận việc mua, bán, chia, tách,

## 3.3 Đơn vị trực tiếp quản lý tài sản CNTT: Là Đơn vị được quyền đưa ra các quyết định về việc: thiết lập, thay đổi, khai thác và chấm dứt hoạt động của tài sản CNTT hoặc một dịch vụ CNTT cụ thể;

**AI trả lời:** Đánh giá: \*\*Cần xem xét thêm\*\*  
  
Lý do:  
  
\* Định nghĩa "Đơn vị trực tiếp quản lý tài sản CNTT" có vẻ chung chung và có thể dẫn đến nhiều cách hiểu khác nhau. Nó tập trung vào quyền đưa ra quyết định về tài sản CNTT, nhưng không rõ ràng về trách nhiệm thực tế trong việc quản lý, vận hành và bảo trì tài sản đó.  
\* Thông tin được cung cấp về tổ chức quản lý hệ thống thông tin từ cấp độ 3 trở lên và tổ chức chỉ có hệ thống thông tin từ cấp độ 2 trở xuống cho thấy sự phân cấp trách nhiệm rõ ràng hơn về an toàn thông tin. Định nghĩa này cần được xem xét trong bối cảnh đó để đảm bảo sự nhất quán và tránh chồng chéo trách nhiệm.  
  
Gợi ý sửa đổi:  
  
Cần làm rõ hơn về các khía cạnh sau:  
  
\* \*\*Trách nhiệm cụ thể:\*\* Bổ sung các trách nhiệm cụ thể của đơn vị này, ví dụ: quản lý rủi ro an ninh mạng, triển khai các biện pháp bảo mật, giám sát hoạt động của hệ thống, ứng phó sự cố, v.v.  
\* \*\*Mối quan hệ với bộ phận chuyên trách an toàn thông tin:\*\* Nếu tổ chức có bộ phận chuyên trách an toàn thông tin (theo quy định cho hệ thống thông tin cấp độ 3 trở lên), cần làm rõ mối quan hệ và phân công trách nhiệm giữa đơn vị quản lý tài sản CNTT và bộ phận này. Ví dụ, đơn vị quản lý tài sản CNTT chịu trách nhiệm triển khai các biện pháp bảo mật do bộ phận an toàn thông tin đề xuất.  
\* \*\*Phân cấp quản lý:\*\* Làm rõ hơn về phân cấp quản lý tài sản CNTT trong tổ chức. Ví dụ, đơn vị này có quyền quyết định về tài sản CNTT trong phạm vi nào? Có cần phê duyệt từ cấp cao hơn không?  
  
Ví dụ về sửa đổi (chỉ là một gợi ý):  
  
"\*\*Đơn vị trực tiếp quản lý tài sản CNTT:\*\* Là đơn vị được giao trách nhiệm quản lý, vận hành và bảo trì một hoặc nhiều tài sản CNTT hoặc dịch vụ CNTT cụ thể, bao gồm việc đưa ra các quyết định về thiết lập, thay đổi, khai thác và chấm dứt hoạt động của tài sản/dịch vụ đó. Đơn vị này chịu trách nhiệm triển khai các biện pháp bảo mật theo hướng dẫn của bộ phận chuyên trách an toàn thông tin (nếu có) và tuân thủ các quy định về an toàn thông tin của tổ chức."

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 47. Trung tâm Điều hành an ninh mạng**  
1. Tổ chức quản lý trực tiếp hệ thống thông tin từ cấp độ 3 trở lên phải thành lập hoặc chỉ định bộ phận chuyên trách để quản lý vận hành Trung tâm Điều hành an ninh mạng (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, tổ chức tài chính vi mô, quỹ tín dụng nhân dân cơ sở, công ty thông tin tín dụng, Công ty Quản lý tài sản của các tổ chức tín dụng Việt Nam, Nhà máy in tiền quốc gia).

**Điều 13. Tổ chức nguồn nhân lực**  
2. Tổ chức chỉ có hệ thống thông tin từ cấp độ 2 trở xuống chỉ định bộ phận có trách nhiệm đảm bảo an toàn thông tin.  
  
3. Tổ chức quản lý trực tiếp hệ thống thông tin từ cấp độ 3 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 toàn thông tin cho tổ chức;

**Điều 55. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước**  
c) Chủ trì, phối hợp với các đơn vị liên quan thuộc Ngân hàng Nhà nước xử lý các vướng mắc phát sinh trong quá trình triển khai thực hiện Thông tư này.  
  
2. Vụ Thanh toán có trách nhiệm phối hợp với Cục Công nghệ thông tin kiểm tra việc thực hiện Thông tư này tại các tổ chức cung ứng dịch vụ trung gian thanh toán.

#### Luat\_tin\_dung.docx

**Điều 152. Phá sản tổ chức tín dụng được kiểm soát đặc biệt**  
3. Phương án chi trả tiền gửi của khách hàng là cá nhân;  
  
4. Lộ trình thực hiện và trách nhiệm triển khai phương án phá sản.  
  
Điều 152c. Tổ chức thực hiện phương án phá sản  
  
1. Ngân hàng Nhà nước chỉ đạo, kiểm tra, giám sát việc triển khai thực hiện phương án phá sản đã được phê duyệt, bao gồm cả việc yêu cầu tổ chức tín dụng được kiểm soát đặc biệt nộp đơn yêu cầu Tòa án mở thủ tục phá sản theo quy định của pháp luật về phá sản.

**Điều 150. Giải thể tổ chức tín dụng được kiểm soát đặc biệt**  
Điều 150a. Tổ chức thực hiện giải thể  
  
1. Sau khi Chính phủ quyết định chủ trương giải thể, Ngân hàng Nhà nước chỉ đạo, kiểm tra, giám sát việc triển khai thực hiện giải thể tổ chức tín dụng được kiểm soát đặc biệt và giám sát việc thanh lý tài sản theo quy định tại khoản 2 Điều 156 của Luật này.  
  
2. Tổ chức tín dụng được kiểm soát đặc biệt thực hiện giải thể theo quy định của pháp luật.  
  
Mục 1đ. PHƯƠNG ÁN CHUYỂN GIAO BẮT BUỘC NGÂN HÀNG THƯƠNG MẠI ĐƯỢC KIỂM SOÁT ĐẶC BIỆT

## 3.4 Người đại diện hợp pháp: Là người đại diện theo pháp luật của NCB trên Giấy phép kinh doanh;

**AI trả lời:** Đánh giá: \*\*Phù hợp\*\*  
  
Lý do:  
  
\* Theo thông tin số 12, "Người đại diện hợp pháp của tổ chức là người đại diện theo pháp luật của tổ chức tín dụng, doanh nghiệp, Tổng giám đốc (Giám đốc) chi nhánh ngân hàng nước ngoài."  
\* Điều 3.4 định nghĩa "Người đại diện hợp pháp: Là người đại diện theo pháp luật của NCB trên Giấy phép kinh doanh".  
\* Như vậy, định nghĩa này phù hợp với quy định chung về người đại diện hợp pháp của tổ chức tín dụng.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 2. Giải thích từ ngữ**  
12. Người đại diện hợp pháp của tổ chức là người đại diện theo pháp luật của tổ chức tín dụng, doanh nghiệp, Tổng giám đốc (Giám đốc) chi nhánh ngân hàng nước ngoài.  
  
13. 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 2. Giải thích từ ngữ**  
11. 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.

#### Luat\_ngan\_hang\_nha\_nuoc.docx

**Điều 53. Quyền, nghĩa vụ của đối tượng thanh tra ngân hàng**  
Điều 53. Quyền, nghĩa vụ của đối tượng thanh tra ngân hàng  
1. Thực hiện kết luận thanh tra.  
  
2. Thực hiện các quyền, nghĩa vụ theo quy định của pháp luật.

#### Luat\_tin\_dung.docx

**Điều 149. Sáp nhập, hợp nhất, chuyển nhượng toàn bộ cổ phần, phần vốn góp của tổ chức tín dụng được kiểm soát đặc biệt**  
b) Có tổ chức tín dụng nhận sáp nhập, hợp nhất, nhà đầu tư nhận chuyển nhượng toàn bộ cổ phần, phần vốn góp đáp ứng các điều kiện theo quy định của pháp luật;  
  
c) Tổ chức tín dụng sau sáp nhập, hợp nhất bảo đảm giá trị thực của vốn điều lệ tối thiểu bằng mức vốn pháp định và đáp ứng các tỷ lệ bảo đảm an toàn quy định tại Điều 130 của Luật này.

**Điều 1. Sửa đổi, bổ sung một số điều của Luật Các tổ chức tín dụng**  
13. Sửa đổi, bổ sung điểm c khoản 1 Điều 54 như sau:  
  
“c) Chịu trách nhiệm trước pháp luật về tính hợp pháp của nguồn vốn góp, mua, nhận chuyển nhượng cổ phần tại tổ chức tín dụng; không sử dụng nguồn vốn do tổ chức tín dụng, chi nhánh ngân hàng nước ngoài cấp tín dụng để mua, nhận chuyển nhượng cổ phần của tổ chức tín dụng; không được góp vốn, mua cổ phần của tổ chức tín dụng dưới tên của cá nhân, pháp nhân khác dưới mọi hình thức, trừ trường hợp ủy thác theo quy định của pháp luật;”

## 3.1. Cấp có thẩm quyền: Là chức danh hoặc người được người đại diện hợp pháp của NCB phân cấp quản lý, phân công, ủy quyền bằng văn bản để thực hiện một hoặc một số chức năng, nhiệm vụ của NCB;

**AI trả lời:** \*\*Đánh giá:\*\* Phù hợp  
  
\*\*Lý do:\*\*  
  
\* Định nghĩa "Cấp có thẩm quyền" trong điều luật cung cấp hoàn toàn tương đồng với định nghĩa "Cấp có thẩm quyền" được quy định tại Khoản 13 của thông tin được cung cấp.  
\* "NCB" được hiểu là tên viết tắt của một tổ chức cụ thể, trong trường hợp này có thể là một tổ chức tín dụng, doanh nghiệp hoặc chi nhánh ngân hàng nước ngoài. Do đó, việc sử dụng khái niệm "người đại diện hợp pháp của NCB" là phù hợp với định nghĩa về người đại diện hợp pháp được nêu trong thông tin (Khoản 12).

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 2. Giải thích từ ngữ**  
12. Người đại diện hợp pháp của tổ chức là người đại diện theo pháp luật của tổ chức tín dụng, doanh nghiệp, Tổng giám đốc (Giám đốc) chi nhánh ngân hàng nước ngoài.  
  
13. 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 13. Tổ chức nguồn nhân lực**  
2. Tổ chức chỉ có hệ thống thông tin từ cấp độ 2 trở xuống chỉ định bộ phận có trách nhiệm đảm bảo an toàn thông tin.  
  
3. Tổ chức quản lý trực tiếp hệ thống thông tin từ cấp độ 3 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 toàn thông tin cho tổ chức;

#### Luat\_tin\_dung.docx

**Điều 146. Thẩm quyền quyết định cơ cấu lại tổ chức tín dụng được kiểm soát đặc biệt**  
b) Phê duyệt phương án phục hồi, sáp nhập, hợp nhất, chuyển nhượng toàn bộ cổ phần, phần vốn góp đối với ngân hàng thương mại, ngân hàng hợp tác xã, công ty tài chính được kiểm soát đặc biệt;  
  
c) Quyết định việc cho vay đặc biệt của Ngân hàng Nhà nước với lãi suất ưu đãi đến mức 0% đối với tổ chức tín dụng được kiểm soát đặc biệt.  
  
3. Ngân hàng Nhà nước có thẩm quyền sau đây:

**Điều 146. Thẩm quyền quyết định cơ cấu lại tổ chức tín dụng được kiểm soát đặc biệt**  
2. Thủ tướng Chính phủ có thẩm quyền sau đây:  
  
a) Quyết định chủ trương cơ cấu lại theo phương án phục hồi, sáp nhập, hợp nhất, chuyển nhượng toàn bộ cổ phần, phần vốn góp đối với ngân hàng thương mại, ngân hàng hợp tác xã, công ty tài chính được kiểm soát đặc biệt;  
  
b) Phê duyệt phương án phục hồi, sáp nhập, hợp nhất, chuyển nhượng toàn bộ cổ phần, phần vốn góp đối với ngân hàng thương mại, ngân hàng hợp tác xã, công ty tài chính được kiểm soát đặc biệt;

**Điều 146. Thẩm quyền quyết định cơ cấu lại tổ chức tín dụng được kiểm soát đặc biệt**  
c) Quyết định việc cho vay đặc biệt của Ngân hàng Nhà nước với lãi suất ưu đãi đến mức 0% đối với tổ chức tín dụng được kiểm soát đặc biệt.  
  
3. Ngân hàng Nhà nước có thẩm quyền sau đây:  
  
a) Quyết định chủ trương cơ cấu lại theo phương án phục hồi, sáp nhập, hợp nhất, chuyển nhượng toàn bộ phần vốn góp đối với quỹ tín dụng nhân dân, tổ chức tài chính vi mô;

## 3.2. Trưởng đơn vị: Giám đốc/Phó Giám đốc Phụ trách tại Khối/Trung tâm độc lập/ĐVKD; QUY CHẾ AN TOÀN THÔNG TIN Mã số: QC.IT.001 Lần ban hành: 01 Tài liệu này chứa các thông tin là tài sản của NCB. Cấm sao chép, in ấn dưới mọi hình thức nếu không được sự cho phép của NCB. 8/48 NCB - Tài liệu nội bộ

**AI trả lời:** Không tìm thấy tài liệu liên quan.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 55. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước**  
Điều 55. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước  
1. Cục Công nghệ thông tin có trách nhiệm:  
  
a) Theo dõi, tổng hợp báo cáo Thống đốc Ngân hàng Nhà nước hàng năm tình hình thực hiện của các tổ chức theo quy định tại Thông tư này;  
  
b) Hàng năm lập kế hoạch kiểm tra việc thực hiện Thông tư này;  
  
c) Chủ trì, phối hợp với các đơn vị liên quan thuộc Ngân hàng Nhà nước xử lý các vướng mắc phát sinh trong quá trình triển khai thực hiện Thông tư này.

**Điều 55. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước**  
4. Ngân hàng Nhà nước chi nhánh tỉnh, thành phố có trách nhiệm thanh tra việc thực hiện Thông tư này tại các tổ chức trên địa bàn và xử lý vi phạm hành chính đối với hành vi vi phạm Thông tư này theo quy định của pháp luật.

#### Luat\_tin\_dung.docx

**Điều 1. Sửa đổi, bổ sung một số điều của Luật Các tổ chức tín dụng**  
15. Sửa đổi, bổ sung điểm c khoản 2 Điều 56 như sau:  
  
“c) Thành viên Hội đồng quản trị, thành viên Ban kiểm soát, Tổng giám đốc (Giám đốc) chuyển nhượng cổ phần cho nhà đầu tư khác nhằm thực hiện phương án cơ cấu lại đã được cấp có thẩm quyền phê duyệt.”  
  
16. Sửa đổi, bổ sung khoản 5 Điều 63 như sau:

**Điều 152. Phá sản tổ chức tín dụng được kiểm soát đặc biệt**  
Trường hợp xây dựng phương án phá sản quỹ tín dụng nhân dân, Ban kiểm soát đặc biệt có trách nhiệm chủ trì, phối hợp với quỹ tín dụng nhân dân được kiểm soát đặc biệt, Bảo hiểm tiền gửi Việt Nam và Ngân hàng Hợp tác xã Việt Nam thực hiện.  
  
2. Trong thời hạn 30 ngày, kể từ ngày nhận được phương án phá sản, Ngân hàng Nhà nước có trách nhiệm xem xét, đánh giá tính khả thi của phương án, trình Chính phủ phê duyệt phương án phá sản tổ chức tín dụng được kiểm soát đặc biệt.

**Điều 1. Sửa đổi, bổ sung một số điều của Luật Các tổ chức tín dụng**  
4. Chủ tịch Hội đồng quản trị, Chủ tịch Hội đồng thành viên, Tổng giám đốc (Giám đốc) của tổ chức tín dụng không được đồng thời là Chủ tịch Hội đồng quản trị, thành viên Hội đồng quản trị, Chủ tịch Hội đồng thành viên, thành viên Hội đồng thành viên, Chủ tịch công ty, Tổng giám đốc (Giám đốc), Phó Tổng giám đốc (Phó giám đốc) hoặc các chức danh tương đương của doanh nghiệp khác.”  
  
8. Bổ sung khoản 4 vào Điều 39 như sau:

## 3.5 Cán bộ nhân viên: Là cá nhân đã ký hợp đồng làm việc tại NCB (bao gồm: Hợp đồng lao động chính thức, Hợp đồng thử việc, Hợp đồng học việc, Hợp đồng cộng tác viên, Hợp đồng khoán gọn, Thỏa thuận thực tập sinh);

**AI trả lời:** Không tìm thấy tài liệu liên quan.

### Tài liệu tham khảo:

#### Luat\_ngan\_hang\_nha\_nuoc.docx

**Điều 9. Cán bộ, công chức của Ngân hàng Nhà nước**  
Điều 9. Cán bộ, công chức của Ngân hàng Nhà nước  
Việc tuyển dụng, sử dụng, quản lý cán bộ, công chức Ngân hàng Nhà nước về nguyên tắc thực hiện theo quy định của Luật cán bộ, công chức. Thủ tướng Chính phủ quy định cơ chế tuyển dụng, chế độ đãi ngộ cán bộ, công chức phù hợp với hoạt động nghiệp vụ đặc thù của Ngân hàng Nhà nước.

**Điều 51. Nguyên tắc thanh tra, giám sát ngân hàng**  
2. Kết hợp thanh tra, giám sát việc chấp hành chính sách, pháp luật về tiền tệ và ngân hàng với thanh tra, giám sát rủi ro trong hoạt động của đối tượng thanh tra, giám sát ngân hàng.  
  
3. Thanh tra, giám sát ngân hàng được thực hiện theo nguyên tắc thanh tra, giám sát toàn bộ hoạt động của tổ chức tín dụng.

#### TT 09\_2020\_TT-NHNN.docx

**Điều 15. Quản lý sử dụng nguồn nhân lực**  
Điều 15. 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 13. Tổ chức nguồn nhân lực**  
Điều 13. 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 toàn thông tin xảy ra tại tổ chức.  
  
2. Tổ chức chỉ có hệ thống thông tin từ cấp độ 2 trở xuống chỉ định bộ phận có trách nhiệm đảm bảo an toàn thông tin.  
  
3. Tổ chức quản lý trực tiếp hệ thống thông tin từ cấp độ 3 trở lên thực hiện:

#### Luat\_tin\_dung.docx

**Điều 146. Thẩm quyền quyết định cơ cấu lại tổ chức tín dụng được kiểm soát đặc biệt**  
6. Số lượng thành viên, nhiệm kỳ Hội đồng quản trị, Hội đồng thành viên, Ban kiểm soát của tổ chức tín dụng được kiểm soát đặc biệt do Ngân hàng Nhà nước quyết định phù hợp với thực trạng hoạt động của tổ chức tín dụng được kiểm soát đặc biệt.

## 3.6 Hệ thống thông tin: Là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng để sản xuất, 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 đơn vị;

**AI trả lời:** Đánh giá: \*\*Cần xem xét thêm\*\*  
  
Lý do:  
  
\* \*\*Tính bao quát:\*\* Định nghĩa về "Hệ thống thông tin" trong Điều 3.6 có vẻ đầy đủ, bao gồm các thành phần cơ bản như phần cứng, phần mềm, cơ sở dữ liệu và mạng. Tuy nhiên, cần xem xét liệu định nghĩa này có bao gồm tất cả các yếu tố cần thiết để mô tả đầy đủ một hệ thống thông tin hiện đại hay không. Ví dụ, có thể cần làm rõ hơn về vai trò của con người (người dùng, quản trị viên) và quy trình trong hệ thống thông tin.  
\* \*\*Tính tương thích với các điều khoản khác:\*\* Cần đảm bảo rằng định nghĩa này tương thích và nhất quán với cách sử dụng thuật ngữ "Hệ thống thông tin" trong các điều khoản khác của văn bản pháp quy này.  
  
Gợi ý sửa đổi (nếu cần thiết sau khi xem xét thêm):  
  
\* Bổ sung yếu tố con người và quy trình vào định nghĩa: "Hệ thống thông tin: Là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu, hệ thống mạng, \*\*con người (người dùng, quản trị viên) và quy trình\*\* để sản xuất, 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 đơn vị."  
\* Rà soát và điều chỉnh các điều khoản khác để đảm bảo tính nhất quán trong cách sử dụng thuật ngữ "Hệ thống thông tin".

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 7. Quản lý tài sản công nghệ 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, hệ quản trị cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển.

**Điều 7. Quản lý tài sản công nghệ thông tin**  
c) Tài sản phần mềm: các phần mềm hệ thống, phần mềm tiện ích, phần mềm lớp giữa, hệ quản trị 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 9, Điều 5 Thông tư này. Định kỳ hàng năm rà soát và cập nhật danh sách tài sản công nghệ thông tin.

**Điều 47. Trung tâm Điều hành an ninh mạng**  
a) Chủ động theo dõi, thu thập, tiếp nhận các thông tin, cảnh báo về các nguy cơ, rủi ro an toàn thông tin từ bên trong và bên ngoài.  
  
b) Xây dựng hệ thống quản lý và phân tích sự kiện an toàn thông tin (SIEM), thực hiện thu thập và lưu trữ tập trung tối thiểu các thông tin: nhật ký của các hệ thống thông tin từ cấp độ 3 trở lên và các hệ thống thông tin có xử lý thông tin cá nhân của khách hàng; cảnh báo, nhật ký của trang thiết bị an ninh mạng (tường lửa, 4 IPS/IDS).

**Điều 20. Trách nhiệm quản lý và quy trình vận hành của tổ chức**  
1. Tổ chức ban hành các quy trình, tài liệu vận hành đối với hệ thống thông tin từ cấp độ 3 trở lên, tối thiểu bao gồm các nội dung: 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

**Điều 7. Quản lý tài sản công nghệ thông tin**  
Điều 7. 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;

## 3.7 Hệ thống thông tin quan trọng: Là hệ thống thông tin khi phát sinh sự cố sẽ làm tổn hại nghiêm trọng đến hoạt động của NCB hoặc làm tổn hại tới lợi ích của khách hàng đang sử dụng dịch vụ của NCB;

**AI trả lời:** Đánh giá: Cần xem xét thêm.  
  
Lý do: Định nghĩa về "Hệ thống thông tin quan trọng" nêu trên mang tính chất chung chung và có thể áp dụng cho nhiều hệ thống khác nhau. Để đánh giá mức độ phù hợp, cần xem xét thêm các yếu tố sau:  
  
\* \*\*Tiêu chí cụ thể:\*\* Cần có các tiêu chí cụ thể, định lượng để xác định mức độ "tổn hại nghiêm trọng" đến hoạt động của NCB hoặc "tổn hại tới lợi ích của khách hàng". Ví dụ: số lượng khách hàng bị ảnh hưởng, mức độ gián đoạn dịch vụ, thiệt hại về tài chính, v.v.  
\* \*\*Phân loại hệ thống:\*\* Cần xác định rõ các hệ thống thông tin nào của NCB được coi là "quan trọng" dựa trên các tiêu chí đã được xác định.  
\* \*\*Mối liên hệ với các quy định khác:\*\* Cần xem xét mối liên hệ giữa định nghĩa này với các quy định khác liên quan đến an toàn thông tin, bảo mật dữ liệu và quản lý rủi ro của NCB.  
  
Gợi ý sửa đổi:  
  
\* Bổ sung các tiêu chí cụ thể, định lượng để xác định mức độ "tổn hại nghiêm trọng" và "tổn hại tới lợi ích của khách hàng".  
\* Liệt kê hoặc phân loại các hệ thống thông tin cụ thể của NCB được coi là "quan trọng".  
\* Đảm bảo định nghĩa này phù hợp và nhất quán với các quy định khác của NCB liên quan đến an toàn thông tin và quản lý rủi ro.  
  
Ví dụ: "Hệ thống thông tin quan trọng là hệ thống thông tin khi phát sinh sự cố sẽ gây ra một trong các hậu quả sau: (1) Gián đoạn dịch vụ cho hơn X% khách hàng trong thời gian Y giờ; (2) Gây thiệt hại tài chính cho NCB vượt quá Z tỷ đồng; (3) Vi phạm nghiêm trọng các quy định về bảo mật dữ liệu cá nhân theo quy định của pháp luật."

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 2. Giải thích từ ngữ**  
2. Sự cố an toàn thông tin là việc thông tin số, hệ thống thông tin bị tấn công hoặc bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng của thông tin.  
  
3. 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.

**Điều 48. Hoạt động ứng cứu sự cố an toàn thông tin**  
4. Nguyên tắc quản lý, sử dụng thông tin trong hoạt động điều phối và ứng cứu sự cố:  
  
a) Thông tin được trao đổi, cung cấp trong quá trình điều phối và ứng cứu sự cố là thông tin bí mật;  
  
b) Nghiêm cấm tổ chức, cá nhân sử dụng thông tin trao đổi trong quá trình điều phối và ứng cứu sự cố để làm ảnh hưởng đến uy tín, hình ảnh của tổ chức cung cấp thông tin.  
  
Mục 9. BẢO ĐẢM HOẠT ĐỘNG LIÊN TỤC CỦA HỆ THỐNG THÔNG TIN

**Điều 51. Xây dựng quy trình, kịch bản bảo đảm hoạt động liên tục**  
1. Xây dựng quy trình xử lý các tình huống mất an toàn, gián đoạn hoạt động của từng cấu phần trong hệ thống thông tin từ cấp độ 3 trở lên.  
  
2. Đối với các tổ chức có cả hệ thống thông tin chính và dự phòng đặt ngoài lãnh thổ Việt Nam phải xây dựng phương án bảo đảm hoạt động liên tục trong trường hợp bị gián đoạn đường truyền kết nối với các hệ thống thông tin chính và dự phòng.

**Điều 41. Quản lý sự thay đổi hệ thống thông tin**  
2. Kiểm tra, đánh giá tác động để bảo đảm hệ thống thông tin hoạt động ổn định, an toàn trên môi trường mới đối với hệ thống thông tin từ cấp độ 3 trở lên khi thay đổi phiên bản hoặc thay đổi hệ điều hành, hệ quản trị cơ sở dữ liệu, phần mềm lớp giữa.

**Điều 19. An toàn tài sản vật lý**  
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

## 3.8 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;

**AI trả lời:** Đánh giá: \*\*Phù hợp\*\*  
  
Lý do: Định nghĩa về thiết bị di động trong điều luật, quyết định, quy định hoặc quy chế được cung cấp hoàn toàn trùng khớp với định nghĩa được cung cấp trong thông tin (mục 5).

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 2. Giải thích từ ngữ**  
4. 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.  
  
5. 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.

**Điều 11. Quản lý sử dụng thiết bị di động**  
Điều 11. 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.

**Điều 11. Quản lý sử dụng thiết bị di động**  
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;

**Điều 11. Quản lý sử dụng thiết bị di động**  
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, tổ chức 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;

**Điều 18. Yêu cầu đối với trung tâm dữ liệu**  
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. Hệ thống chữa cháy bảo đảm khi chữa cháy không làm hư hỏng thiết bị lắp đặt bên trong, trừ trường hợp tổ chức có hệ thống dự phòng bảo đảm an toàn tuyệt đối cho dữ liệu và có khả năng thay thế hoàn toàn hệ thống chính trong vòng 01 giờ.  
  
8. Có hệ thống sàn kỹ thuật hoặc lớp cách ly chống nhiễm điện; hệ thống tiếp địa.

## 3.9 Vật mang tin: Là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin số;

**AI trả lời:** \*\*Đánh giá:\*\* Phù hợp  
  
\*\*Lý do:\*\* Định nghĩa về "Vật mang tin" trong Điều 3.9 hoàn toàn trùng khớp với định nghĩa được cung cấp trong thông tin tham khảo (mục 6). Cụ thể, cả hai đều xác định vật mang tin là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin số.  
  
\*\*Gợi ý sửa đổi:\*\* Không cần thiết.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 2. Giải thích từ ngữ**  
6. Vật mang tin là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin số.  
  
7. Tường lửa là tập hợp các thành phần hay một hoặc một số 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.

**Điều 12. Quản lý sử dụng vật mang tin**  
Điều 12. Quản lý sử dụng vật mang tin  
Tổ chức phải quản lý sử dụng vật mang tin theo quy định sau:  
  
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 9. Quản lý tài sản vật lý**  
5. 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.

**Điều 19. An toàn tài sản vật lý**  
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 7. Quản lý tài sản công nghệ 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, hệ quản trị cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển.

## 3.10 Dữ liệu nhạy cảm: Là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị;

**AI trả lời:** \*\*Đánh giá:\*\* Cần xem xét thêm  
  
\*\*Lý do:\*\*  
  
\* \*\*Thông tin lưu hành nội bộ:\*\* Định nghĩa này có sự tương đồng với khái niệm "Thông tin riêng (hoặc thông tin nội bộ)" đã được định nghĩa trong thông tin tham khảo. Tuy nhiên, cần làm rõ phạm vi và cách thức quản lý thông tin này để đảm bảo tính nhất quán.  
\* \*\*Ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị:\*\* Tiêu chí này mang tính định tính và khó xác định một cách khách quan. Cần có các tiêu chí cụ thể hơn để đánh giá mức độ ảnh hưởng.  
\* \*\*Thiếu sự liên kết với thông tin cá nhân:\*\* Định nghĩa "Dữ liệu nhạy cảm" không đề cập đến thông tin cá nhân, trong khi thông tin cá nhân cũng có thể được coi là nhạy cảm và cần được bảo vệ.  
  
\*\*Gợi ý sửa đổi:\*\*  
  
1. \*\*Bổ sung tham chiếu đến thông tin cá nhân:\*\* "Dữ liệu nhạy cảm là dữ liệu bao gồm thông tin mật, thông tin riêng (hoặc thông tin nội bộ) của đơn vị hoặc do đơn vị quản lý, \*\*và thông tin cá nhân của khách hàng\*\*, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị hoặc gây tổn hại đến quyền riêng tư của cá nhân."  
2. \*\*Làm rõ tiêu chí đánh giá mức độ ảnh hưởng:\*\* Bổ sung các tiêu chí cụ thể để đánh giá mức độ ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị (ví dụ: mức độ thiệt hại về tài chính, số lượng khách hàng bị ảnh hưởng, mức độ gián đoạn hoạt động).  
3. \*\*Đảm bảo tính nhất quán với các định nghĩa khác:\*\* Rà soát và điều chỉnh định nghĩa để đảm bảo tính nhất quán với các định nghĩa khác trong văn bản, đặc biệt là định nghĩa về "Thông tin riêng (hoặc thông tin nội bộ)" và "Thông tin cá nhân".

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 4. Phân loại thông tin**  
2. Thông tin riêng (hoặc thông tin nội bộ) là thông tin được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng được xác định danh tính;  
  
3. Thông tin cá nhân là thông tin định danh khách hàng và các thông tin sau đây: thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch và các thông tin có liên quan khác;

**Điều 47. Trung tâm Điều hành an ninh mạng**  
a) Chủ động theo dõi, thu thập, tiếp nhận các thông tin, cảnh báo về các nguy cơ, rủi ro an toàn thông tin từ bên trong và bên ngoài.  
  
b) Xây dựng hệ thống quản lý và phân tích sự kiện an toàn thông tin (SIEM), thực hiện thu thập và lưu trữ tập trung tối thiểu các thông tin: nhật ký của các hệ thống thông tin từ cấp độ 3 trở lên và các hệ thống thông tin có xử lý thông tin cá nhân của khách hàng; cảnh báo, nhật ký của trang thiết bị an ninh mạng (tường lửa, 4 IPS/IDS).

**Điều 7. Quản lý tài sản công nghệ 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, hệ quản trị cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển.

**Điều 33. Các yêu cầu khi sử dụng dịch vụ của bên thứ ba**  
1. Đánh giá rủi ro công nghệ thông tin, rủi ro hoạt động tối thiểu bao gồm các nội dung sau:  
  
a) Nhận diện rủi ro, phân tích, ước lượng cấp độ tổn hại, mối đe dọa đến an toàn thông tin;  
  
b) Khả năng kiểm soát các quy trình nghiệp vụ, khả năng cung cấp dịch vụ liên tục, khả năng thực hiện nghĩa vụ cung cấp thông tin cho các cơ quan nhà nước;  
  
c) Xác định rõ vai trò, trách nhiệm của các bên liên quan trong việc bảo đảm chất lượng dịch vụ;

**Điều 2. Giải thích từ ngữ**  
3. 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.  
  
4. 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.

## 3.11 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;

**AI trả lời:** \*\*Đánh giá:\*\* Phù hợp  
  
\*\*Lý do:\*\* Định nghĩa về tường lửa được cung cấp trong điều luật, quyết định, quy định hoặc quy chế này hoàn toàn trùng khớp với định nghĩa được cung cấp trong thông tin tham khảo.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 2. Giải thích từ ngữ**  
6. Vật mang tin là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin số.  
  
7. Tường lửa là tập hợp các thành phần hay một hoặc một số 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.

**Điều 23. Quản lý an toàn, bảo mật hệ thống mạng**  
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 của tổ chức;  
  
d) Có giải pháp kiểm soát, phát hiện và ngăn chặn kịp thời các kết nối, truy cập trái phép vào hệ thống mạng nội bộ của tổ chức có hệ thống thông tin từ cấp độ 3 trở lên;

**Điều 18. Yêu cầu đối với trung tâm dữ liệu**  
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 cấp độ 3 trở lên phải được bảo vệ, giám sát 24/7.

**Điều 17. Yêu cầu chung đối với nơi lắp đặt trang thiết bị công nghệ thông tin**  
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 của hệ thống thông tin từ cấp độ 3 trở lên 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 29. Quản lý truy cập mạng nội bộ**  
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 mạng không tin cậy vào mạng nội bộ của tổ chức bảo đảm an toàn thông tin.  
  
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.

## 3.12 Điểm yếu về mặt kỹ thuật: Là thành phần/vị trí trong hệ thống CNTT dễ bị khai thác, lợi dụng khi bị tấn công hoặc xâm nhập bất hợp pháp;

**AI trả lời:** \*\*Đánh giá:\*\* Phù hợp  
  
\*\*Lý do:\*\*  
  
\* Định nghĩa "Điểm yếu về mặt kỹ thuật" trong Điều 3.12 hoàn toàn tương đồng với định nghĩa được nêu trong Điều 43 của tài liệu tham khảo: "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."  
  
\*\*Gợi ý sửa đổi:\*\* Không cần thiết.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 43. Quản lý các điểm yếu về mặt kỹ thuật**  
Điều 43. Quản lý các điểm yếu về mặt kỹ thuật  
Tổ chức quản lý các điểm yếu về mặt kỹ thuật như sau:  
  
1. Xây dựng quy định về việc đánh giá, quản lý và kiểm soát các điểm yếu về mặt kỹ thuật của các hệ thống thông tin đang sử dụng.  
  
2. Thường xuyên cập nhật thông tin liên quan đến lỗ hổng, điểm yếu về mặt kỹ thuật.  
  
3. Thực hiện dò quét lỗ hổng, điểm yếu của các hệ thống thông tin định kỳ theo quy định tại khoản 3 Điều 42 hoặc khi tiếp nhận được thông tin liên quan đến lỗ hổng, điểm yếu mới.

**Điều 43. Quản lý các điểm yếu về mặt kỹ thuật**  
3. Thực hiện dò quét lỗ hổng, điểm yếu của các hệ thống thông tin định kỳ theo quy định tại khoản 3 Điều 42 hoặc khi tiếp nhận được thông tin liên quan đến lỗ hổng, điểm yếu mới.  
  
4. Đánh giá cấp độ tác động, rủi ro của từng lỗ hổng, điểm yếu về mặt kỹ thuật được phát hiện của các hệ thống thông tin đang sử dụng và đưa ra phương án, kế hoạch xử lý.  
  
5. Xây dựng, tổ chức triển khai các giải pháp xử lý, khắc phục và báo cáo kết quả xử lý.

**Điều 2. Giải thích từ ngữ**  
3. 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.  
  
4. 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.

**Điều 7. Quản lý tài sản công nghệ thông tin**  
c) Tài sản phần mềm: các phần mềm hệ thống, phần mềm tiện ích, phần mềm lớp giữa, hệ quản trị 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 9, Điều 5 Thông tư này. Định kỳ hàng năm rà soát và cập nhật danh sách tài sản công nghệ thông tin.

**Điều 24. Trao đổi thông tin**  
4. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp.  
  
5. 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.

## 3.13 Tính bảo mật của thông tin: Là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng;

**AI trả lời:** Đánh giá: \*\*Phù hợp\*\*  
  
Lý do: Định nghĩa về "Tính bảo mật của thông tin" được cung cấp hoàn toàn phù hợp với các nguyên tắc chung về bảo mật thông tin, cũng như các quy định về bảo vệ thông tin bí mật được đề cập trong tài liệu. Cụ thể, tài liệu nhấn mạnh việc bảo vệ thông tin bí mật, hạn chế truy cập trái phép, và mã hóa thông tin trước khi trao đổi. Định nghĩa này nhấn mạnh việc kiểm soát quyền truy cập, đảm bảo chỉ những người được ủy quyền mới có thể tiếp cận thông tin, điều này hoàn toàn tương thích với các biện pháp bảo vệ được mô tả trong tài liệu.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 4. Phân loại thông tin**  
4. Thông tin bí mật là: (i) Thông tin Mật, Tối Mật, Tuyệt Mật theo quy định của pháp luật về bảo vệ bí mật nhà nước; (ii) Thông tin hạn chế tiếp cận theo quy định của tổ chức.

**Điều 26. Giám sát và ghi nhật ký hoạt động của hệ thống thông tin**  
3. Có phương án giám sát, cảnh báo khi có thay đổi thông tin bí mật lưu trên hệ thống lưu trữ/phương tiện lưu trữ của các hệ thống thông tin từ cấp độ 4 trở lên.  
  
4. Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, thay đổi và truy cập trái phép; bảo đảm người quản trị hệ thống và người sử dụng không thể xóa hay sửa đổi nhật ký hệ thống ghi lại các hoạt động của chính họ.  
  
5. Thực hiện việc đồng bộ thời gian giữa các hệ thống thông tin.

**Điều 24. Trao đổi thông tin**  
3. Các thông tin bí mật phải được mã hóa hoặc áp dụng các biện pháp bảo mật thông tin trước khi trao đổi. Đối với hệ thống thông tin cấp độ 5, tổ chức phải sử dụng kết nối mạng an toàn và các thiết bị, phương tiện chuyên dụng để mã hóa, giải mã thông tin bí mật và khi trao đổi thông tin.  
  
4. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp.

**Điều 2. Giải thích từ ngữ**  
2. Sự cố an toàn thông tin là việc thông tin số, hệ thống thông tin bị tấn công hoặc bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng của thông tin.  
  
3. 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.

#### Luat\_ngan\_hang\_nha\_nuoc.docx

**Điều 38. Bảo vệ bí mật thông tin**  
Điều 38. Bảo vệ bí mật thông tin  
1. Ngân hàng Nhà nước có trách nhiệm lập danh mục, thay đổi độ mật, giải mật bí mật nhà nước về lĩnh vực tiền tệ và ngân hàng gửi cơ quan nhà nước có thẩm quyền quyết định; bảo vệ bí mật của Ngân hàng Nhà nước và của tổ chức, cá nhân theo quy định của pháp luật.

## 3.14 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;

**AI trả lời:** Đánh giá: \*\*Phù hợp\*\*  
  
Lý do: Định nghĩa về "Tính toàn vẹn của thông tin" trong điều luật, quyết định, quy định hoặc quy chế được cung cấp hoàn toàn phù hợp với mục tiêu bảo vệ sự chính xác và đầy đủ của thông tin, đồng thời kiểm soát quyền thay đổi thông tin. Điều này tương ứng với định nghĩa chung về tính toàn vẹn trong an toàn thông tin.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 4. Phân loại thông tin**  
4. Thông tin bí mật là: (i) Thông tin Mật, Tối Mật, Tuyệt Mật theo quy định của pháp luật về bảo vệ bí mật nhà nước; (ii) Thông tin hạn chế tiếp cận theo quy định của tổ chức.

**Điều 2. Giải thích từ ngữ**  
2. Sự cố an toàn thông tin là việc thông tin số, hệ thống thông tin bị tấn công hoặc bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng của thông tin.  
  
3. 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.

**Điều 35. Hợp đồng sử dụng dịch vụ với bên thứ ba**  
1. Cam kết của bên thứ ba về bảo đảm an toàn thông tin bao gồm:  
  
a) Không sao chép, thay đổi, sử dụng hay cung cấp dữ liệu của tổ chức sử dụng dịch vụ cho cá nhân, tổ chức khác, trừ trường hợp có yêu cầu của cơ quan nhà nước có thẩm quyền theo quy định của pháp luật; trong trường hợp này, bên thứ ba phải thông báo cho tổ chức sử dụng dịch vụ trước khi cung cấp dữ liệu, trừ khi việc thông báo sẽ vi phạm pháp luật Việt Nam;

**Điều 37. Yêu cầu về an toàn, bảo mật các hệ thống thông tin**  
1. Xây dựng tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin. Trong đó các yêu cầu về an toàn, bảo mật được xây dựng đồng thời với việc xây dựng các yêu cầu kỹ thuật, nghiệp vụ.  
  
2. Xây dựng phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu. Kết quả kiểm tra phải lập thành báo cáo và được cấp có thẩm quyền phê duyệt trước khi đưa vào vận hành chính thức.

**Điều 4. Phân loại thông tin**  
Điều 4. Phân loại thông tin  
Thông tin xử lý, lưu trữ thông qua hệ thống thông tin được phân loại theo thuộc tính bí mật như sau:  
  
1. 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;  
  
2. Thông tin riêng (hoặc thông tin nội bộ) là thông tin được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng được xác định danh tính;

## 3.15 Tính sẵn sàng của thông tin: Là đảm bảo những người được cấp quyền có thể truy xuất thông tin ngay khi có nhu cầu;

**AI trả lời:** Không tìm thấy tài liệu liên quan.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 30. Quản lý truy cập hệ thống thông tin và ứng dụng**  
3. Quản lý và phân quyền truy cập thông tin và ứng dụng bảo đảm 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.  
  
4. Các hệ thống thông tin sử dụng chung nguồn tài nguyên phải được cấp có thẩm quyền phê duyệt.

**Điều 33. Các yêu cầu khi sử dụng dịch vụ của bên thứ ba**  
1. Đánh giá rủi ro công nghệ thông tin, rủi ro hoạt động tối thiểu bao gồm các nội dung sau:  
  
a) Nhận diện rủi ro, phân tích, ước lượng cấp độ tổn hại, mối đe dọa đến an toàn thông tin;  
  
b) Khả năng kiểm soát các quy trình nghiệp vụ, khả năng cung cấp dịch vụ liên tục, khả năng thực hiện nghĩa vụ cung cấp thông tin cho các cơ quan nhà nước;  
  
c) Xác định rõ vai trò, trách nhiệm của các bên liên quan trong việc bảo đảm chất lượng dịch vụ;

**Điều 4. Phân loại thông tin**  
2. Thông tin riêng (hoặc thông tin nội bộ) là thông tin được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng được xác định danh tính;  
  
3. Thông tin cá nhân là thông tin định danh khách hàng và các thông tin sau đây: thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch và các thông tin có liên quan khác;

**Điều 24. Trao đổi thông tin**  
4. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp.  
  
5. 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.

**Điều 47. Trung tâm Điều hành an ninh mạng**  
a) Chủ động theo dõi, thu thập, tiếp nhận các thông tin, cảnh báo về các nguy cơ, rủi ro an toàn thông tin từ bên trong và bên ngoài.  
  
b) Xây dựng hệ thống quản lý và phân tích sự kiện an toàn thông tin (SIEM), thực hiện thu thập và lưu trữ tập trung tối thiểu các thông tin: nhật ký của các hệ thống thông tin từ cấp độ 3 trở lên và các hệ thống thông tin có xử lý thông tin cá nhân của khách hàng; cảnh báo, nhật ký của trang thiết bị an ninh mạng (tường lửa, 4 IPS/IDS).

## 3.16 An ninh mạng: Là sự bảo vệ hệ thống CNTT và thông tin truyền đưa trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính toàn vẹn, tính bảo mật và tính sẵn sàng của thông tin;

**AI trả lời:** Không tìm thấy tài liệu liên quan.

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 23. Quản lý an toàn, bảo mật hệ thống mạng**  
Điều 23. 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:

**Điều 31. Quản lý kết nối Internet**  
3. Triển khai các giải pháp an ninh mạng tại các cổng kết nối Internet để bảo đảm an toàn trước các hiểm họa tấn công từ Internet vào mạng nội bộ của tổ chức.  
  
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 tổ chức thông qua cổng kết nối Internet.  
  
Mục 6. QUẢN LÝ SỬ DỤNG DỊCH VỤ CÔNG NGHỆ THÔNG TIN CỦA BÊN THỨ BA

**Điều 31. Quản lý kết nối Internet**  
c) Các hành vi bị cấm, hạn chế;  
  
d) Kiểm soát kết nối, truy cập sử dụng Internet;  
  
đ) Các biện pháp bảo đảm an toàn thông tin khi kết nối Internet.  
  
2. Thực hiện quản lý tập trung, thống nhất các cổng kết nối Internet trong toàn bộ tổ chức.  
  
3. Triển khai các giải pháp an ninh mạng tại các cổng kết nối Internet để bảo đảm an toàn trước các hiểm họa tấn công từ Internet vào mạng nội bộ của tổ chức.

**Điều 32. Các nguyên tắc chung về sử dụng dịch vụ của bên thứ ba**  
2. Không làm suy giảm việc kiểm soát quy trình nghiệp vụ của tổ chức.  
  
3. Không làm thay đổi trách nhiệm của tổ chức trong việc bảo đảm an toàn thông tin.  
  
4. Dịch vụ công nghệ thông tin của bên thứ ba phải đáp ứng các quy định về bảo đảm an toàn thông tin của tổ chức.

**Điều 48. Hoạt động ứng cứu sự cố an toàn thông tin**  
2. Mạng lưới có nhiệm vụ phối hợp các nguồn lực trong và ngoài ngành ứng phó hiệu quả sự cố an toàn thông tin, góp phần bảo đảm hệ thống ngân hàng hoạt động an toàn.  
  
3. Nguyên tắc trong hoạt động điều phối và ứng cứu sự cố

## 3.17 Thông tin dữ liệu: Là một loại tài sản có thể tồn tại dưới nhiều hình thức như bản giấy in hoặc viết tay, dạng số hóa có thể được lưu chuyển qua đường bưu điện, qua các thiết bị điện tử hoặc qua lời nói.

**AI trả lời:** Đánh giá: Cần xem xét thêm  
  
Lý do: Định nghĩa "Thông tin dữ liệu" trong điều 3.17 có đề cập đến "dạng số hóa có thể được lưu chuyển qua đường bưu điện, qua các thiết bị điện tử hoặc qua lời nói". Tuy nhiên, theo thông tin được cung cấp, "Tài sản thông tin" (điều 7.1.a) bao gồm "các dữ liệu, thông tin ở dạng số được xử lý, lưu trữ thông qua hệ thống thông tin". Như vậy, phạm vi của "Thông tin dữ liệu" có vẻ rộng hơn "Tài sản thông tin" vì nó bao gồm cả thông tin không được xử lý hoặc lưu trữ qua hệ thống thông tin (ví dụ: lời nói). Cần xem xét thêm để đảm bảo sự thống nhất và rõ ràng giữa các định nghĩa.  
  
Gợi ý sửa đổi: Cần làm rõ mối quan hệ giữa "Thông tin dữ liệu" và "Tài sản thông tin". Có thể sửa đổi định nghĩa "Thông tin dữ liệu" để phù hợp hơn với phạm vi của "Tài sản thông tin" hoặc bổ sung thêm các quy định về quản lý "Thông tin dữ liệu" không thuộc phạm vi "Tài sản thông tin".

### Tài liệu tham khảo:

#### TT 09\_2020\_TT-NHNN.docx

**Điều 7. Quản lý tài sản công nghệ 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, hệ quản trị cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển.

**Điều 7. Quản lý tài sản công nghệ thông tin**  
Điều 7. 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;

**Điều 9. Quản lý tài sản vật lý**  
Điều 9. Quản lý tài sản vật lý  
1. 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 11, Điều 12 Thông tư này.  
  
2. Với mỗi hệ thống thông tin do tổ chức trực tiếp quản lý, tổ chức 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.

**Điều 7. Quản lý tài sản công nghệ thông tin**  
c) Tài sản phần mềm: các phần mềm hệ thống, phần mềm tiện ích, phần mềm lớp giữa, hệ quản trị 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 9, Điều 5 Thông tư này. Định kỳ hàng năm rà soát và cập nhật danh sách tài sản công nghệ thông tin.

**Điều 8. Quản lý tài sản thông tin**  
Điều 8. Quản lý tài sản thông tin  
1. Với mỗi hệ thống thông tin, tổ chức 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 loại thông tin quy định tại 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.