**NỘI DUNG GỢI Ý GÓP Ý DỰ THẢO THÔNG TƯ VỀ BẢO MẬT HỆ THỐNG CÔNG NGHỆ**

**THÔNG TIN TRONG HOẠT ĐỘNG NGÂN HÀNG**

***(Tập trung vào những điểm mới so với quy định hiện hành)***

**Đơn vị góp ý: ……………………………………………………**

**Góp ý có thể tập trung (nhưng không giới hạn) vào các vấn đề sau:**

* Các nội dung quy định có **hợp lý** không, nếu không, vui lòng nêu lý do; Các vấn đề khác dự kiến phát sinh **vướng mắc** khi văn bản được triển khai thực hiện;
* **Đề xuất, kiến nghị** nhằm hoàn thiện các quy định chưa phù hợp.

**Phương thức góp ý: theo đường Công văn hoặc điền vào mẫu dưới đây.**

Để có thể góp ý được đầy đủ và chính xác, rất mong Quý Doanh nghiệp/Hiệp hội theo dõi toàn văn Dự thảo đăng tải trên website của VCCI tại địa chỉ: www.vibonline.com.vn - Mục Dự thảo.

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **VẤN ĐỀ** | **NỘI DUNG DỰ THẢO** | **Ý KIẾN GÓP Ý** |
| **1** | **Tổ chức nguồn nhân lực** | **-** Thủ trưởng đơn vị hoặc 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 sự cố an toàn thông tin mạng xảy ra tại đơn vị  - Đơn vị sở hữu hoặc trực tiếp vận hành hệ thống thông tin cấp độ 3 trở lên phải: 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 mạng cho đơn vị.; quản lý vận hành Trung tâm điều hành an ninh mạnh đáp ứng yêu cầu quy định tại Điều 45 Thông tư này (sẽ được tóm tẳt bên dưới) |  |
| **2** | **Sao lưu dự phòng** | - Đối với hệ thống thông tin từ cấp 2 trở lên, đơn vị phải có phương án sử dụnh hệ thống hoặc phương tiện lưu trữ độc lập sao lưu dự phòng các dữ liệu quan trọng trên máy chủ.  - Hệ thống thông tin từ cấp độ 3 trở lên phải có phương án tự động sao lưu theo định kỳ hàng ngày và kết quả sao lưu phải được lưu thành hai bản; phải kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu 6 tháng/ lần. |  |
| **3** | **Quản lý sử dụng dịch vụ công nghệ thông tin của bên thứ ba** | - Việc sử dụng dịch vụ công nghệ thông tin không làm suy giảm khả năng cung cấp dịch vụ liên tục của đơn vị cho khách hàng hay việc kiểm soát quy trình nghiệp vụ của đơn vị, hoặc làm thay đổi trách nhiệm của đơn vị trong việc bảo đảm an toàn, bảo mật thông tin; bên thứ ba không được thực hiện toàn bộ công việc bảo đảm an toàn, bảo mật thông tin; Đánh giá rủi ro trước khi sủ dựng dịch vụ công nghệ thông tin gồm các nội dung tối thiểu sau: Nhận diện ruti ro phân tích ước lượng mức độ tổn hại, mối đe doạ đến an toàn, bảo mật hệ thống công nghệ thông tin; Khả năng kiểm soát các quy trình nghiệp vụ, cung cấp dịch vụ liên tục cho khách hàng, và thực hiện nghĩa vụ cung cấp thông tin cho Ngân hàng Nhà nước; xác định rõ vài tò, trách nhiệm các bên; xây dựng biện pháp giảm rủi ro và phòng ngừa, ứng cứu, khắc phục sự cố  - Trường hợp sử dụng dịch vụ điện toán đám mây, đơn vị phải: Phân loại hoạt động, nghiệp vụ dự kiến triển khai trên điện toán đám mây dựa trên đánh giá tác động của hoạt động nghiệp vụ đó với hoạt động của đơn vị. Đối với các cấu phần của hệ thống thông tin từ cấp độ 3 trở lên thì đơn vị phải có phuwong án dự phòng.  - Dự án phải được kiểm thử và đánh giá sẵn sàng thay thế cho các hoạt động nghiệp vụ triển khai trên điện toán đám mây, rà soát bổ sung áp dụng các biện pháp bảo đảm an toàn bảo mật thông tin của đơn vị giới hạn truy cập từ điện toán đám mây đến các hệ thống thông tin của đơn vị.  - Trường hợp đơn vị sử dụng dịch vụ điện toán đám mây của bên thứ ba bên ngoài lãnh thổ Việt Nam phục vụ cho hệ thống thông tin từ cấp độ 2 trở lên, cần bổ sung tiêu chí: Chính sách, điều kiện kinh tế và pháp lý của quốc gia/vùng lãnh thổ nơi bên thứ ba đăng ký kinh doanh và lấy ý kiến đánh giá về pháp lý đối với các điều khoản tại hợp đồng của ít nhất một (01) tổ chức tư vấn pháp lý hợp pháp có kinh nghiệm tư vấn các hợp đồng quốc tế, vị trí cụ thể của các trung tâm dữ liệu (thành phố, quốc gia).  - Hợp đồng sử dụng dịch vụ:  + Bên thứ ba cam kết đáp ứng điều 33 Thông tư này; Không sao chép, thay đổi, sử dụng hay cung cấp dữ liệu của đơn vị cho các bên khác, trừ khi thực hiện theo yêu cầu của pháp luật Việt Nam và phải thông báo chơ đơn vị trước khi cung cấp dữ liệu trừ khi thôngbaso sẽ vi phạm pháp luật Việt Nam; Dữ liệu phát sinh trong quá trình sử dụng dịch vụ là tài sản của đơn vị, khi chấm dứt: bên thứ ba thực hiện hoàn trả lại toàn bộ dữ liệu triển khai và dữ liệu phát sinh trong quá trình sử dụng dịch vụ, cam kết hoàn thành việc xoá toàn bộ dữ liệu của đơn vị trong một khoảng thời gian xác định.  +Đối với hợp đồng sử dụng điện toán đám mây: Bên thứ ba phải cung cấp báo cáo kiểm toán tuân thủ công nghệ thông tin do tổ chức kiểm toán độc lập thực hiện hàng năm trong thời gian thực hiện hợp đồng, cung cấp: (i) Công cụ kiểm soát chất lượng dịch vụ đám mây; (ii) Quy trình giám sát, kiểm soát chất lượng dịch vụ đám mây, minh bạch các vị trí (thành phố, quốc gia) đặt trung tâm dữ liệu bên ngoài lãnh thổ Việt Nam triển khai dịch vụ cho đơn vị, trách nhiệm bảo vệ dữ liệu , chống truy cập trái phép, hỗ trợ hợp tác điều tra trong trường hợp có yêu cần từ các cơ quan chức năng của Việt Nam theo quy định của pháp luật, Dữ liệu của đơn vị phải được tách biệt với dữ liệu khác sử dụng cùng nền tảng kỹ thuật do bên thứ ba cung cấp.  - Đối với hệ thống thông tin từ cấp độ 3 trở lên hoặc hệ thống thông tin sử dụng dịch vụ điện toán đám mây, phải đánh giá sự tuân thủ các quy định về bảo đảm an toàn bảo mật công nghệ thông tin của bên thứ ba theo đúng thỏa thuận đã ký kết. Thực hiện đánh giá sự tuân thủ định kỳ hàng năm hoặc đột xuất khi có nhu cầu. Việc đánh giá tuân thủ có thể sử dụng kết quả kiểm toán công nghệ thông tin của tổ chức kiểm toán độc lập. |  |
| **4** | **Quản lý bảo trì hệ thống** | Đơn vị phải tổ chức thực hiện bảo trì ngay sau khi đưa hệ thống thông tin vào vận hành chính thức. Định kỳ thực hiện bảo trì tối thiểu 6 tháng một lần đối với hệ thống thông tin từ cấp độ 3 trở lên, mỗi năm một lần đối với các hệ thống thông tin khác; rà soát, cập nhật tiêu chuẩn, định mức, yêu cầu kỹ thuật quy định về quản lý công tác bảo trì, bảo dưỡng trang thiết bị công nghệ thông tin tối thiểu mỗi năm một lần hoặc khi có sự thay đổi đối với hệ thống thông tin. |  |
| **5** | **Quản lý và ứng cứu sự cố an toàn thông tin mạng** | Trung tâm điều hành an ninh mạng phải thực hiện nhiệm vụ: Xây dựng hệ thống giám sát an toàn mạng (SIEM) nhằm thu thập và lưu trữ tập trung các thông tin tối thiểu: nhật ký của các hệ thống thông tin cấp độ 3 trở lên; cảnh báo/nhật ký của trang thiết bị an ninh mạng (tường lửa, IPS/IDS); phải gửi cảnh báo theo thời gian thực đến người quản trị hệ thống khi phát hiện sự cố liên quan đến các hệ thống: (i) Hệ thống thông tin phục vụ khách hàng yêu cầu hoạt động 24/7; (ii) Hệ thống cung cấp giao dịch trực tuyến; (iii) Hệ thống thông tin từ cấp độ 4 trở lên. |  |
| **6** | **Kiểm soát và khắc phục sự cố** | Lập danh sách sự cố an toàn thông tin mạng và phương án xử lý sự cố đối với các hệ thống thông tin từ cấp độ 2 trở lên. Tối thiểu 6 tháng một lần thực hiện rà soát, cập nhật danh sách, phương án ứng cứu sự cố. |  |