|  |  |  |
| --- | --- | --- |
| Logo VRB_mau chuan | **NGÂN HÀNG LIÊN DOANH**  **VIỆT-NGA**  Số: 01823/CV-VRB | **CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *Hà Nội, ngày 07 tháng 11 năm 2024* |

**BÁO CÁO KẾT QUẢ THỰC HIỆN TĂNG CƯỜNG AN TOÀN THÔNG TIN HỆ THỐNG PHẦN MỀM CITAD TẠI VRB**

| **STT** | **Các yêu cầu kiểm soát an toàn thông tin** | **Yêu cầu** | | **Hiện trạng tuân thủ tại thành viên** |
| --- | --- | --- | --- | --- |
| **Bắt buộc** | **Khuyến nghị** |
| **1. Bảo vệ an toàn môi trường hoạt động** | | | | |
| 1.1 | Hạn chế truy cập Internet | | | |
| *1.1.1* | *Hạn chế truy cập Internet* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Toàn bộ máy chủ không có kết nối Internet. * Máy của cán bộ vận hành không có kết nối Internet   Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| 1.2 | Bảo vệ các hệ thống thông tin quan trọng với môi trường CNTT dùng chung | | | |
| *1.2.1* | *Bảo mật môi trường CITAD* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Hệ thống CITAD được đặt trong vùng Server Farm của VRB. Vùng Server Farm được kiểm soát bời tường lửa. * Các thành phần của hệ thống được phân tách theo quy hoạch hạ tầng mạng và được kiểm soát bởi tường lửa. * Kiểm soát truy cập hệ thống từ người dùng bằng tưởng lửa, xác thực địa chỉ MAC của người dùng. * Quản trị hệ thống thông qua máy chủ trung gian.   Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| *1.2.2* | *Kiểm soát tài khoản đặc quyền của hệ điều hành* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Tài khoản quản trị hệ thống được tạo tài khoản tương quyền. * Có hệ thống lưu nhật ký tập trung * Định kỳ thực hiện đổi mật khẩu quản trị.   ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| *1.2.3* | *Bảo vệ môi trường ảo hóa* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Hệ thống CITAD được cài đặt trên môi trường ảo hóa. * Hạ tầng máy chủ Ảo hóa được đặt tại trung tâm dữ liệu CMC. * Kết nối hạ tầng máy chủ của hệ thống được kiểm soát bởi tường lửa.   ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| 1.3 | Giảm bề mặt tấn công và các lỗ hổng | | | |
| *1.3.1* | *Cập nhật bảo mật* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Định kỳ VRB có tổ chức thực hiện pentest hệ thống. Đánh giá các rủi ro của hệ thống và xem xét thực hiện cập nhật các rủi ro.   ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| *1.3.2* | *Nâng cao bảo mật hệ thống* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Hạ tầng máy chủ, tường lửa, thiết bị mạng được đặt tại trung tâm dữ liệu CMC. Trung tâm dữ liệu CMC đạt chuẩn Uptime Tier 3 – TIA942 Rated 3. * Chỉ tạo tài khoản cho cán bộ sử dụng. * Trên máy chủ không cài các phần mềm không liên quan và không cho phép sử dụng USB.   ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| *1.3.3* | *Bảo vệ luồng dữ liệu truyền bên ngoài* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Thực hiện backup dữ liệu hàng ngày và lưu trữ cả online và offline. * Định kỳ thực hiện khôi phục dữ liệu.   ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| *1.3.4* | *Kiểm soát giao dịch* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  - Triển khai hệ thống đối soát, giám sát nội địa.  - Hạn chế truy cập hệ thống CITAD ngoài giờ làm viêc, cảnh báo khi đăng nhập hệ thống ngoài giờ làm việc.  - Thực hiện duyệt điện thủ công với những giao dịch giá trị lớn, thực hiện đối soát hàng ngày.  - Giám sát thông tin người gửi, người thụ hưởng thuộc danh sách đáng ngờ,… thông việc quét điện trên hệ thống phòng chống rửa tiền.  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| *1.3.5* | *Nâng cao bảo mật ứng dụng* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Thay đổi các mật khẩu truy cập mặc định; * Định kỳ rà soát và disable các tài khoản không sử dụng. * chỉ cho phép cán bộ có thẩm quyền truy cập hệ thống. * chỉ cho phép kết nối từ máy tính tại đơn vị; * không cài đặt các chương trình hoặc ứng dụng không cần thiết; * định kỳ rà soát và xem xét cập nhật bản vá.   ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| 1.4 | Bảo mật vật lý môi trường hoạt động | | | |
| *1.4.1* | *An toàn vật lý* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * USB Token được sử dụng trong môi trường bảo mật. Máy chủ được đặt tại trung tâm dữ liệu và có khóa cho vùng dữ liệu riêng. * Thiết bị backup được lưu trữ tại khu vực riêng của Hội Sở Chính và có khóa an toàn. * Máy truy cập được trang bị các biện pháp bảo đảm an toàn thông tin. Có joindomain và cấm sử dụng USB.   ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| **2. Kiểm soát và giới hạn các truy cập** | | | | |
| 2.1 | Ngăn chặn xâm phạm thông tin đăng nhập | | | |
| *2.1.1* | *Xác thực đa thành tố* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:   * Đối với người dùng quản trị hệ thống: truy cập qua máy chủ Jump và xác thực đa yếu tố. * Đối với người dùng cuối: Xác thực địa chỉ MAC.   ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| 2.2 | Quản trị định danh và các đặc quyền | | | |
| *2.2.1* | *Thẩm tra nhân sự* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Xác minh lý lịch tư pháp của quản bộ quản trị hệ thống.  ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| *2.2.2* | *Lưu trữ mật khẩu theo hình thức vật lý hoặc logic* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |
| **3. Ứng phó sự cố an ninh mạng** | | | |  |
| 3.1 | Kế hoạch ứng phó sự cố an ninh mạng | | | |
| *3.2.1* | *Lập kế hoạch ứng phó sự cố an ninh mạng* |  |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Ban hành quy định xử lý sự cố CNTT. Số 00316a/2021/QĐ-CN ngày 31/03/2021  ….……………………………..................................................................  Kế hoạch thực hiện: ….……………………………..................................................................  Khác  Mô tả: ….……………………………................................................................... |