|  |  |  |
| --- | --- | --- |
| D:\CONG VIEC\VRB\THIET KE\logo chuan nhat.jpg | **NGÂN HÀNG LIÊN DOANH VIỆT-NGA**    Số: …../CV-VRB  *(V/v: Báo cáo thực hiện hướng dẫn tăng cường ATTT hệ thống phần mềm CITAD của VRB)* | **CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *Hà Nội, ngày … tháng 12 năm 2022* |

**Kính gửi: Cục Công nghệ thông tin**

Căn cứ theo Công văn số 1942/CNTT6 V/v “Báo cáo thực hiện Hướng dẫn tăng cường an toàn thông tin hệ thống phần mềm CITAD tại thành viên Hệ thống TTĐTLNH”. Ngân hàng liên doanh Việt - Nga xin báo cáo Cục Công nghệ thông tin về việc thực hiện tăng cường ATTT hệ thống phần mềm CITAD của VRB (theo phụ lục đính kèm).

Mọi thông tin cần trao đổi xin gửi về Ban Công nghệ ngân hàng điện tử - Ngân hàng Liên doanh Việt - Nga, theo địa chỉ: Tòa nhà số 75 Trần Hưng Đạo, Phường Trần Hưng Đạo, Hoàn Kiếm, Hà Nội. Điện thoại: 024.39426668, Fax: 024.39426669 hoặc gửi email về địa chỉ [it@vrbank.com.vn](mailto:it@vrbank.com.vn).

Ngân hàng Liên doanh Việt – Nga xin chân thành cảm ơn./.

|  |  |
| --- | --- |
| ***Nơi nhận:***  *- Như đề gửi;*  *- Lưu Ban CNNHĐT, VP.* | **KT. TỔNG GIÁM ĐỐC**  **PHÓ TỔNG GIÁM ĐỐC**  **Ivanov Sergey Pavlovich** |

**Báo cáo tăng cường an toàn thông tin**

**hệ thống phần mềm CITAD**

| **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 | Han chế truy cập Internet | | | |
| 1.1.1 | Hạn chế truy cập Internet | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Các máy chủ vận hành chuyên dùng, các máy chủ trung gian và các thành phần có liên quan đến CITAD nằm trong vùng an toàn, chặn truy cập Internet và truy cập email.  Các máy trạm vận hành chung áp dụng chính sách hạn chế truy cập Internet, chỉ truy cập một số địa chỉ URL thuộc danh sách thông qua Proxy.  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 | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Các máy chủ của hệ thống CITAD được đặt trong vùng Server Farm, chặn truy cập Internet và truy cập email. Tách biệt với môi trường kiểm thử. Được bảo vệ bởi Firewall.  Kế hoạch thực hiện:      Khác  Mô tả: |
| 1.2.2 | Kiểm soát tài khoản đặc quyền của hệ điều hành | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  VRB có chính sách quản lý tài khoản đặc quyền. Việc sử dụng tài khoản đặc quyền hệ điều hành được kiểm soát và chỉ sử dụng để cài đặt, cấu hình hệ thống.  Kế hoạch thực hiện:      Khác  Mô tả: |
| 1.2.3 | Bảo vệ môi trường ảo hóa | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  VRB chỉ sử dụng môi trường vật lý cho hệ thống CITAD  Kế hoạch thực hiện:    Khác  Mô tả: |
| 1.3 | Giảm bề mặt tấn công và các lỗ hỏng | | | |
| 1.3.1 | Cập nhật bảo mật | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Tất cả phần cứng và phần mềm đều trong giai đoạn hỗ trợ của nhà cung cấp, thực hiện thường xuyên nâng cấp bắt buộc và áp dụng các bản cập nhật an ninh cần thiết (Các bản cập nhật luôn được xác thực nguồn gốc và kiểm tra tính toàn vẹn)  Kế hoạch thực hiện:      Khác  Mô tả: |
| 1.3.2 | Nâng cao bảo mật hệ thống | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Tất cả các hệ thống luôn tuân thủ hướng dẫn bảo mật của nhà sản xuất, tiêu chuẩn bảo mật nội bộ, áo dụng quá trình nâng cao bảo mật.  Tài liệu hóa quy trình vận hành và cấu hình tối ưu hệ thống  Thường xuyên áp dụng các thiết lập bảo mật cho hệ thống  Kế hoạch thực hiện:    Khác  Mô tả: |
| 1.3.3 | Bảo vệ luông dữ liệu bên ngoài |  | X | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Khi sao chép hoặc trích xuất dữ liệu nhậy cảm của hệ thống CITAD luôn sử dụng biện pháp mã hóa và bảo vệ bằng mật khẩu.  Định kỳ khôi phục dữ liệu liên quan đến hệ thống CITAD.  Kế hoạch thực hiện:      Khác  Mô tả: |
| 1.3.4 | Kiểm soát giao dịch |  | X | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Chỉ cho phép truy cập trong giờ làm việc  Luôn giám sát các giao dịch bất thường  Đối chiếu giao dịch cuối ngày  Kế hoạch thực hiện:      Khác  Mô tả: |
| 1.3.5 | Nâng cao bảo mật ứng dụng | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Mật khẩu truy cập mặc định đã được thay đổi  Vô hiệu hóa các tài khoản người dùng không cần thiết  Vô hiệu hóa các phương thức kết nối không cần thiết  Cấu hình an toàn các kết nối từ xa  Loại bỏ các gói, chương trình hoặc ứng dụng không cần thiết.  Tinh chỉnh/thay đổi cấu hình mặc định  Kế hoạch thực hiện:      Khác  Mô tả: |
| 1.4 | Bảo mật vật ký môi trường hoạt động | | | |
| 1.4.1 | An toàn vật lý | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:      Kế hoạch thực hiện:    Khác  Mô tả: |
| 1. **Kiểm soát và giới hạn các truy cập** | | | | |
| 2.1 | Ngăn ngừa xâm phạm thông tin đăng nhập | | | |
| 2.1.1 | Xác thực đa thành tố |  | X | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:      Kế hoạch thực hiện:    Khác  Mô tả: |
| 2.2 | Quản trị định danh và các đặc quyền | | | |
| 2.2.1 | Thẩm tra nhân sự | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Nhân sự được xác minh lý lịch, xác minh lý lịch tư pháp.  Kế hoạch thực hiện:      Khác  Mô tả: |
| 2.2.2 | Lưu trữ mật khẩu theo hình thức vật lý hoặc logic | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  Mật khẩu được bảo vệ theo hình thức số hóa, mã hóa toàn bộ, chỉ sử dụng cho người được phân quyền.  Kế hoạch thực hiện:      Khác  Mô tả: |
| 1. **Ứng phó sự cố an ninh mạng** | | | | |
| 3.2.1 | Lập kế hoạch ứng phó sự cố an ninh mạng | X |  | Tuân thủ hoàn toàn  Chưa tuân thủ  Hiện trạng:  VRB đã ban hành “Quy trình ứng phó xử lý sự cố an ninh mạng”  Kế hoạch thực hiện:      Khác  Mô tả: |