## Thông tin về công ty sinh viên tham gia thực tập:

### Trình tự phát triển phần mềm của VAB:

#### Các giai đoạn phát triển phần mềm nghiệp vụ:

1. Lập kế hoạch.
2. Khảo sát yêu cầu người sử dụng.
3. Phân tích yêu cầu hệ thống.
4. Thiết kế phần mềm.
5. Lập trình phần mềm.
6. Kiểm tra, thử nghiệm phần mềm.
7. Triển khai thí điểm.
8. Đào tạo, tập huấn.
9. Đóng gói, bàn giao phần mềm.
10. Triển khai chính thức.
11. Nghiệm thu phần mềm.
12. Hỗ trợ vận hành.

#### Đối với các phần mềm nghiệp vụ thực hiện theo yêu cầu cấp bách được Ban Tổng Giám đốc phê duyệt, đơn vị chủ trì công nghệ thông tin được quyết định trình tự rút gọn, có thể không bao gồm các giai đoạn quy định tại các điểm a, b, g, i tại khoản 1.2.2.1.

### Quy định các nguyên tắc lập trình chương trình ứng dụng của VAB:

#### Quy định về chứng thực người dùng: Các hệ thống phải chứng thực người dùng qua LDAPs. Người dùng sử dụng username/password của email cá nhân do VietABank cung cấp để đăng nhập vào ứng dụng sau khi được phân quyền.

#### Quy định về theo dõi nhật ký người dùng đăng nhập: ứng dụng phải có khả năng theo dõi nhật ký người dùng đăng nhập (login) và thoát ra khỏi hệ thống (logout). Đối với các bảng dữ liệu quan trọng, ứng dụng phải có nhật ký theo dõi người dùng khi thêm dữ liệu, người dùng cập nhật dữ liệu, dữ liệu cũ trước khi cập nhật và dữ liệu mới sau khi cập nhật.

#### Về xem và in báo cáo:

##### Người dùng chỉ được phép xem và in dữ liệu của đơn vị mình, không được phép xem và in dữ liệu của đơn vị khác.

##### Chi nhánh có thể xem và in số liệu của chính Chi nhánh, xem và in số liệu của Phòng giao dịch trực thuộc bất kỳ trực thuộc mà mình quản lý.

##### Người dùng của Hội sở chính khi được phân quyền thì được phép xem và in báo cáo của một đơn vị bất kỳ.

1. Xem và in báo cáo số liệu toàn hàng.
2. Xem và in báo cáo một Chi nhánh bất kỳ.
3. Xem và in báo cáo một chi nhánh bất kỳ bao gồm số liệu các Phòng giao dịch trực thuộc.
4. Xem và in số liệu một Phòng giao dịch bất kỳ.

#### Phân quyền người dùng theo vai trò (role): Ứng dụng cho phép phân quyền theo nhóm người dùng. Số nhóm người dùng là không giới hạn.

#### Về đơn vị:

1. Các đơn vị trong ngân hàng đều có mã đơn vị do Khối Quản trị Nguồn Nhân Lực quy định. Mã này có 7 byte AAABBCD với quy định như sau:
2. Đối với Trụ sở chính: có bốn cấp gồm cấp một là Trụ sở chính (3 byte đầu), cấp hai là khối (5 byte đầu), cấp 3 là phòng ban (6 byte đầu), cấp 4 là bộ phận (7 byte).
3. Đối với chi nhánh: Có hai cấp gồm cấp một, cấp hai, cấp ba đều là chi nhánh. Cấp bốn là phòng ban.
4. Đối với Phòng giao dịch: Có hai cấp gồm cấp một, cấp hai, cấp ba đều là phòng giao dịch. Cấp bốn là bộ phận.

#### Font Unicode: Các chương trình ứng dụng có dữ liệu là chữ có dấu Tiếng Việt thì thống nhất sử dụng loại font chữ Unicode.

#### Chương trình phải dùng tên Domain name không được dùng IP: Các chương trình ứng dụng phải sử dụng domain name, không được sử dụng địa chỉ IP trong các khai báo kết nối, cấu hình đường dẫn chương trình.

#### Các công cụ lập trình phát triển không được cài lên máy chủ của ứng dụng: Các công cụ lập trình phát triển không được cài lên máy chủ của ứng dụng để hạn chế các rủi ro có thể xảy ra khi bị tấn công chiếm quyền điều khiển.

#### Chương trình được kiểm tra an ninh trước khi triển khai: Chương trình ứng dụng phải được kiểm tra và xác nhận về mặt an ninh trước khi triển khai chính thức. Việc kiểm tra an ninh sẽ do Phòng An ninh Thông tin thuộc Khối CNNH thực hiện.

#### Quy định số lẻ trong các phép toán: các phép tính trong các chương trình liên quan đến tiền tệ cách làm tròn số như sau:

1. Đối với VNĐ: Làm tròn không có số lẻ (làm tròn đến hàng đơn vị) hoặc theo mô tả cụ thể của đơn vị yêu cầu.
2. Đối với ngoại tệ USD, EUR, v.v…: làm tròn hai số lẻ hoặc theo mô tả cụ thể của đơn vị yêu cầu.
3. Đối với vàng XAU: làm tròn ba số lẻ hoặc theo mô tả cụ thể của đơn vị yêu cầu.

#### Ngôn ngữ lập trình và cơ sở dữ liệu: Các chương trình ứng dụng mới phải sử dụng ngôn ngữ lập trình Java và cơ sở dữ liệu là Oracle. Các trường hợp ngoại lệ phải được sự chấp thuận của lãnh đạo khối CNNH.

#### Định danh người dùng: Người dùng được phân quyền sử dụng trong chương trình phải xác định được cụ thể là Tài khoản quản trị ứng dụng/ tài khoản người sử dụng/ tài khoản khai thác dữ liệu; tránh và hạn chế việc phân quyền, định danh tên tài khoản chung chung như Admin, Quantri, v.v…

#### Các thông tin bắt buộc phải có trong cở sở dữ liệu: MSNV, tài khoản email, đơn vị và các thông tin khác để có thể tích hợp vào chương trình quản lý User tập trung.

#### Các bảng dữ liệu phải có vùng ghi chú: Khi thiết kế và lập trình các bảng dữ liệu phải có cột ghi chú để người dùng có thể nhập thông tin bổ sung, diễn giải khác.

#### Cơ sở dữ liệu test và phát triển ứng dụng: phải được đặt trên hệ thống test quy định của Ngân hàng và tách biệt với môi trường hệ thống thật. Khi bắt đầu dự án, người phụ trách dự án phải yêu cầu được lãnh đạo phê duyệt đến IT Helpdesk để yêu cầu cấp phát cơ sở dữ liệu dùng để test hoặc phát triển ứng dụng.

### Các chuẩn mã hóa của VAB:

* Dữ liệu được mã hóa/giải mã và được lưu trữ trên hệ thống máy tính cần có:
  + Độ dài khóa của Hệ thống mã hóa đối xứng phải tối thiểu là 128 bit;
  + Các khóa mã hóa bất đối xứng phải có độ dài với độ mạnh tương đương nhau.
* Dữ liệu được mã hóa/giải mã bởi hệ thống ứng dụng dịch vụ truyền tải qua môi trường mạng cần phải sử dụng:
  + Chứng chỉ số máy chủ web và các máy chủ web hỗ trợ công nghệ SSLv3/TLSv1 với chế độ mã hóa mạnh (mã hóa đối xứng 128 bit hoặc cao hơn, mã hóa bất đối xứng 2048 bit hoặc cao hơn)
  + Đối với tài nguyên phục vụ công cộng: sử dụng các chứng chỉ số phải được chứng nhận bởi các tổ chức tin cậy (Verisign EV SSL Certificate);
  + Đối với tài nguyên phục vụ nội bộ: sử dụng các chứng chỉ số tự chứng nhận để quản lý tài nguyên.
* Sử dụng SSLv3 để bảo vệ các dịch vụ/giao thức truyền tải dữ liệu không được mã hóa;
* Sử dụng SSHv2 kết hợp sử dụng public/private keys để kết nối và xác thực từ xa;
* Sử dụng thuật toán AES-128, AES-256 để mã hóa bảo vệ thông tin nhạy cảm;
* Sử dụng PKCS#7, PKCS#12, PKCS#1 để trao đổi thông tin đối tác;
* Sử dụng Radmin (AES-256 bit) để quản trị và hỗ trợ kỹ thuật từ xa;
* Sử dụng IPSec (VPN) để bảo vệ kênh làm việc từ xa;
* Sử dụng WPA2 (chuẩn bảo mật Wireless LAN) cho mạng không dây;
* Các thuật toán chuẩn và đã được chứng minh độ an toàn phải đóng vai trò nền tảng trong các công nghệ mã hóa được sử dụng bởi VietABank.
* Việc sử dụng các thuật toán mã hóa tự thiết kế không đươc sử dụng vào bất kỳ mục đích nào, trừ khi được phê duyệt bởi Ban giám đốc.