Số: ......./2022/TTr-CNTT *Hà Nội, ngày tháng 01 năm 2022*



**NGÂN HÀNG TMCP XĂNG DẦU PETROLIMEX**

Trụ sở chính: Tầng 16, 23, 24 Tòa nhà Mipec, số 229 Tây Sơn, P.Ngã Tư Sở, Q. Đống Đa, TP. Hà Nội

ĐT: 024.62811298 - Fax: 024.62811299 - Web: [www.pgbank.com.vn](http://www.pgbank.com.vn)

**TỜ TRÌNH**

*V/v Triển khai Quản lý kết nối Internet tập trung*

*Tại Hội Sở và các Chi nhánh tại Hà Nội*

**Kính gửi: Tổng Giám Đốc**

Thực hiện chỉ đạo của Tổng Giám đốc, Khối CNTT đã hoàn thành triển khai hệ thống Quản lý kết nối Internet tập trung (còn gọi là hệ thống Proxy Internet). Áp dụng thực tế tại Khối CNTT cho thấy hệ thống hoạt động hiệu quả, chính sách cấu hình linh hoạt và giám sát được các kết nối ra Internet của người dùng cũng như từ các máy chủ, nâng cao an toàn thông tin của hệ thống và đáp ứng tuân thủ các yêu cầu của Quy chế An toàn thông tin cũng như các quy định về Quản lý kết nối Internet được quy định tại Điều 31, Thông tư 09/2020/TT-NHNN (Quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng).

Để triển khai mở rộng cho người dùng tại Hội Sở và các chi nhánh tại Hà Nội, tiến tới triển khai trên toàn quốc trong năm 2022, nhằm cân bằng giữa mục tiêu đảm bảo an toàn thông tin và mục tiêu phục vụ kinh doanh, Khối CNTT kính trình Tổng Giám đốc phê duyệt chính sách mở kết nối cho người dùng như sau:

1. **Chính sách về các ứng dụng chat OTT**

Các ứng dụng chat OTT (như Zalo, Skype, Facebook Messenger, Viber, Telegram….) sử dụng các giao thức được mã hóa, cho phép người dùng chat và gửi file với nhau mà các hệ thống giám sát không biết được nội dung. Điều này tạo ra nguy cơ thất thoát thông tin ra bên ngoài. Tuy nhiên hiện nay một số bộ phận nghiệp vụ đang sử dụng các ứng dụng này để giao tiếp với khách hàng hoặc đối tác, dẫn đến nhu cầu sử dụng để phục vụ kinh doanh, do đó Khối CNTT đề xuất phê duyệt chính sách:

1. Cho phép chat qua các ứng dụng: Zalo, Skype.
2. Cho phép download file khi bên ngoài gửi file qua các ứng dụng này
3. Không cho phép người dùng gửi file đi qua các ứng dụng này.

**Rủi ro còn lại:** người dùng vẫn có thể gửi các thông tin mật/thông tin nhạy cảm ra bên ngoài dưới dạng text mà hệ thống không giám sát được.

1. **Chính sách về các hệ thống lưu trữ online**

Việc cho phép người dùng được phép sử dụng các hệ thống lưu trữ online (như Fshare, 4share, GoogleDrive, OneDrive sẽ gây ra rủi ro thất thoát thông tin, cũng như dữ liệu của ngân hàng khi lưu trữ trên hệ thống lưu trữ online với tài khoản cá nhân của người dùng sẽ không được thu hồi khi nhân sự nghỉ việc, do đó Khối CNTT đề xuất phê duyệt chính sách:

1. Không cho phép người dùng upload lên các hệ thống lưu trữ/chia sẻ file.
2. Cho phép download file từ các hệ thống chia sẻ file này trừ một số trường hợp file download về có thể gây rủi ro cho an toàn thông tin (như các file thực thi không rõ nguồn gốc, file có dung lượng quá lớn làm quá tải băng thông…). Đối với các trường hợp này, người dùng phải liên hệ với Khối CNTT để trợ giúp download cho các mục đích hợp lệ.
3. Để phục vụ việc trao đổi file có dung lượng lớn khi làm việc với các đối tác, Khối CNTT sẽ phối hợp với đối tác ECM để triển khai tính năng chia sẻ file cho đối tác trên hệ thống ECM. Theo đó, người dùng phải upload file lên ECM và gửi đường link download cho đối tác truy cập. Hệ thống sẽ ghi lại nhật ký tất cả các file được người dùng gửi ra ngoài Ngân hàng phục vụ cho mục đích giám sát an ninh thông tin và truy cứu trách nhiệm cá nhân (nếu có)

**Rủi ro còn lại:** khi nhiều người dùng bên ngoài cùng truy cập có thể làm quá tải hệ thống ECM.

1. **Chính sách về sử dụng email cá nhân**

Các hệ thống email cá nhân (như Gmail, Yahoo mail, Microsoft Outlook email,) tạo ra rủi ro người dùng có thể gửi thông tin ra bên ngoài mà không kiểm soát được, do đó Khối CNTT đề xuất chính sách:

1. Không cho phép người dùng gửi email cá nhân khi sử dụng kết nối qua hệ thống Internet tập trung.
2. Cho phép người dùng được mở email ở chế độ “chỉ đọc” đối với một số nhà cung cáp email mà hệ thống có thể hỗ trợ kiểm soát chặn việc gửi đi, bao gồm:

* Gmail

**Rủi ro còn lại:** không.

1. **Chính sách về các trang mạng xã hội, các trang video Youtube, streaming**

Các trang mạng xã hội như Facebook, Tiktok…, Youtube, streaming… có băng thông lớn, nếu mở sẽ gây quá tải hệ thống, do đó Khối CNTT đề xuất chính sách:

1. Mặc định chặn không truy cập các trang mạng xã hội và video streaming.
2. Mở cho một số đơn vị, cá nhân có chức năng, nhiệm vụ cần sử dụng, bao gồm:

* Phòng Phát triển thương hiệu và mạng lưới.
* Ban Tổng Giám Đốc.

1. Khi cần truyền thông toàn hàng qua mạng xã hội, Phòng PTTH &ML sẽ thông báo cho khối CNTT mở tạm thời trong thời gian truyền thông

**Rủi ro còn lại**: không.

1. **Chính sách về các trang web độc hại/các trang web không phục vụ công việc**

Chính sách đề xuất: Khối CNTT chủ động chặn.

1. **Chính sách về ngoại lệ/báo chặn nhầm/mở thêm các trang web theo yêu cầu của người dùng**

Trong quá trình hoạt động, khi phát sinh các yêu cầu kết nối ngoại lệ người dùng sẽ

* Gửi yêu cầu trên hệ thống Issue Tracking, được phê duyệt bởi trưởng đơn vị (Giám đốc Khối hoặc Giám đốc Chi nhánh hoặc người được ủy quyền).
* Phòng ATTT - Khối CNTT sẽ tiếp nhận yêu cầu và xem xét mức độ ảnh hưởng an toàn. Trong trường hợp kết nối không an toàn hoặc không cần thiết cho công việc Phòng ATTT có quyền từ chối yêu cầu. Trong trường hợp yêu cầu là an toàn và phù hợp với nhu cầu công việc, Phòng ATTT phối hợp để cấu hình hệ thống đáp ứng yêu cầu của người dùng.

1. **Thời gian triển khai và phạm vi triển khai**
2. Thời gian triển khai:

Khối CNTT sẽ triển khai lần lượt cho các Khối/Phòng tại Trụ sở chính và các Chi nhánh tại Hà Nội từ 10/01/2021 đến 31/1/2021.

1. Phạm vi triển khai:

Triển khai áp dụng cho:

* Các Khối/Phòng tại Trụ sở chính.
* Chi nhánh Đông Đô
* Chi nhánh Thăng Long
* Chi nhánh Hà Nội

Kính trình Tổng Giám đốc xem xét phê duyệt.

Trân trọng đề nghị!

|  |  |
| --- | --- |
| **PHÊ DUYỆT CỦA TGĐ** | **Khối CNTT** |
|  |  |