

# Thiết lập bảo mật 2 lớp Enforce 2FA

*(Tài liệu dành cho các sản phẩm Khối HCSN)*

# I.Sự cần thiết của bảo mật 2 lớp Enforce 2FA

Bảo mật 2 lớp là một phương tiện hiệu quả để bảo vệ tài khoản và thông tin cá nhân khỏi các mối đe dọa trực tuyến

## 1.Tăng cường Bảo mật:

-Xác minh hai yếu tố đòi hỏi không chỉ mật khẩu mà còn một yếu tố khác như mã OTP, fingerprint, hoặc mã xác nhận. Điều này làm tăng cường bảo mật, vì người tấn công cần phải vượt qua hai bước để truy cập thông tin.

## 2.Ngăn chặn Truy Cập Trái Phép:

-2FA giúp ngăn chặn người xâm nhập truy cập trái phép vào tài khoản người dùng. Ngay cả khi mật khẩu bị đánh cắp, người tấn công cũng cần mã xác nhận từ yếu tố thứ hai.

## 3.Bảo vệ Thông Tin Cá Nhân:

-Bảo mật 2 lớp là một lớp bảo vệ bổ sung, đảm bảo rằng dữ liệu cá nhân và quan trọng không bị lộ ra ngoài dễ dàng.

## 4.Giảm Rủi Ro Tài Khoản Bị Chiếm Đoạt:

-Mặc dù có thể xảy ra việc mật khẩu bị đánh cắp, nhưng việc có thêm một yếu tố xác minh làm giảm rủi ro tài khoản bị chiếm đoạt đáng kể.

## 5.Tuân Thủ và Điều Chỉnh:

-Đối với các doanh nghiệp và tổ chức, sử dụng bảo mật 2 lớp giúp tuân thủ các quy định và chuẩn mực bảo mật. Nó cũng tạo ra khả năng điều chỉnh theo nhu cầu cụ thể của tổ chức.

## 6.An Toàn Tài Khoản Ngân Hàng và Giao Dịch Trực Tuyến:

-Trong lĩnh vực tài chính, việc áp dụng 2FA là quan trọng để bảo vệ thông tin tài khoản ngân hàng và giao dịch trực tuyến, giảm nguy cơ mất mát tài chính.

## II. Tổng quan về tài liệu

### 1. Mục đích của tài liệu

Mục đích xây dựng quy chuẩn thiết lập Enforce 2FA và xác thực tài khoản để các dự án/sản phẩm thực hiện theo.

### 2. Đối tượng sử dụng

Tài liệu nhằm phục vụ cho các sản phẩm/dự án thực hiện phương thức Enforce 2FA

### 3. Các luồng xây dựng bảo mật 2 lớp Enforce 2FA

- Luồng đổi mật khẩu đối với mật khẩu không đủ bảo mật
- Luồng đối với các tài khoản đã không hoạt động trong 180 ngày đã inactive
- Luồng khuyến nghị bật đối với người dùng chưa bật 2FA
- Luồng xử lý với các user chưa verify thông tin, sau khi login xong phần mềm yêu cầu verify (Email, Mobile) để sau này có thể tự lấy lại pass
- Luồng user Admin bật 2FA cho toàn bộ người dùng

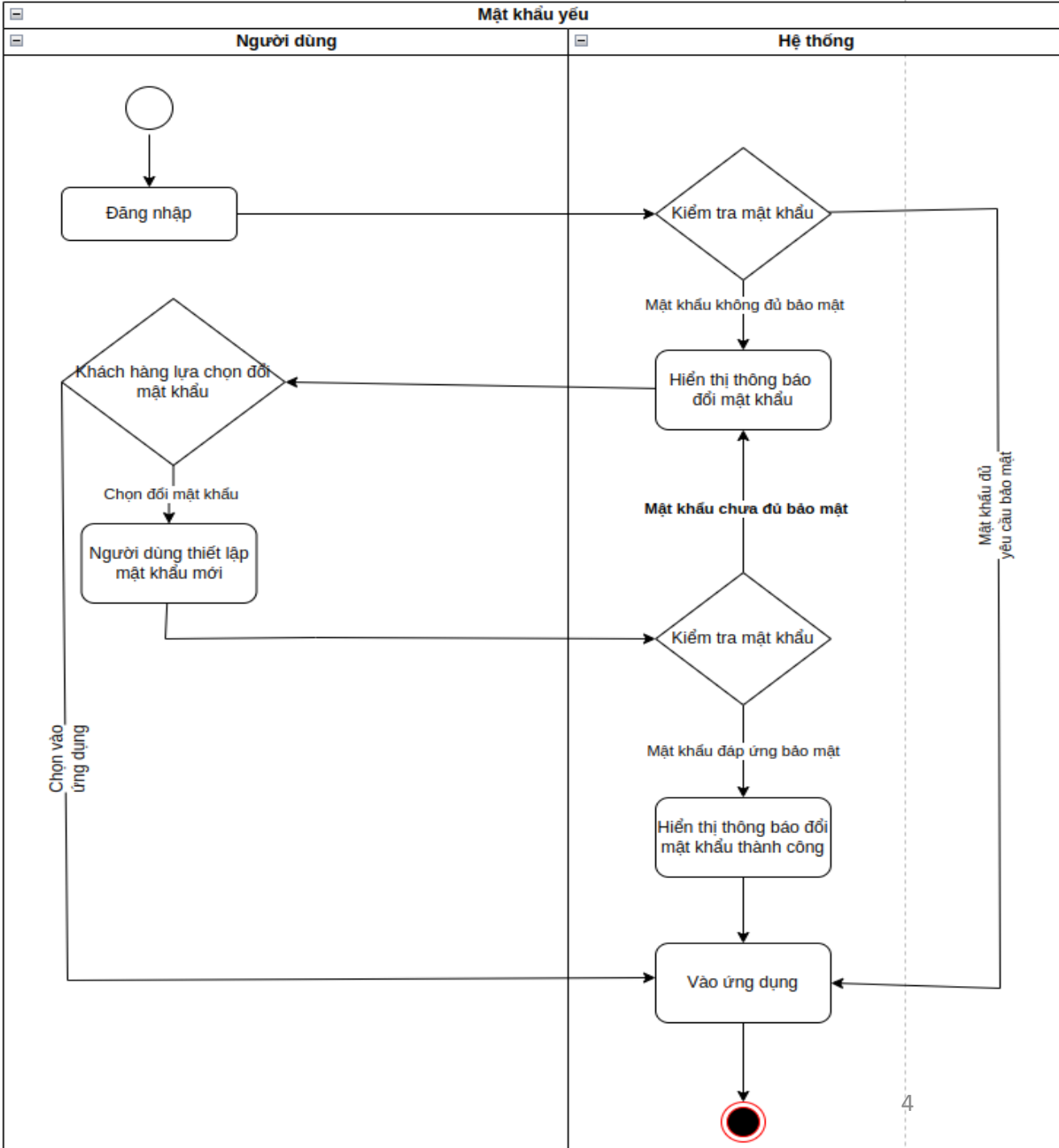
III.ĐẶC TẢ CHI TIẾT CHỨC NĂNG

1. Đối với người dùng đang sử dụng mật khẩu không đủ bảo mật, sau khi đăng nhập vào xong phần mềm cần yêu cầu/khuyến nghị đổi pass

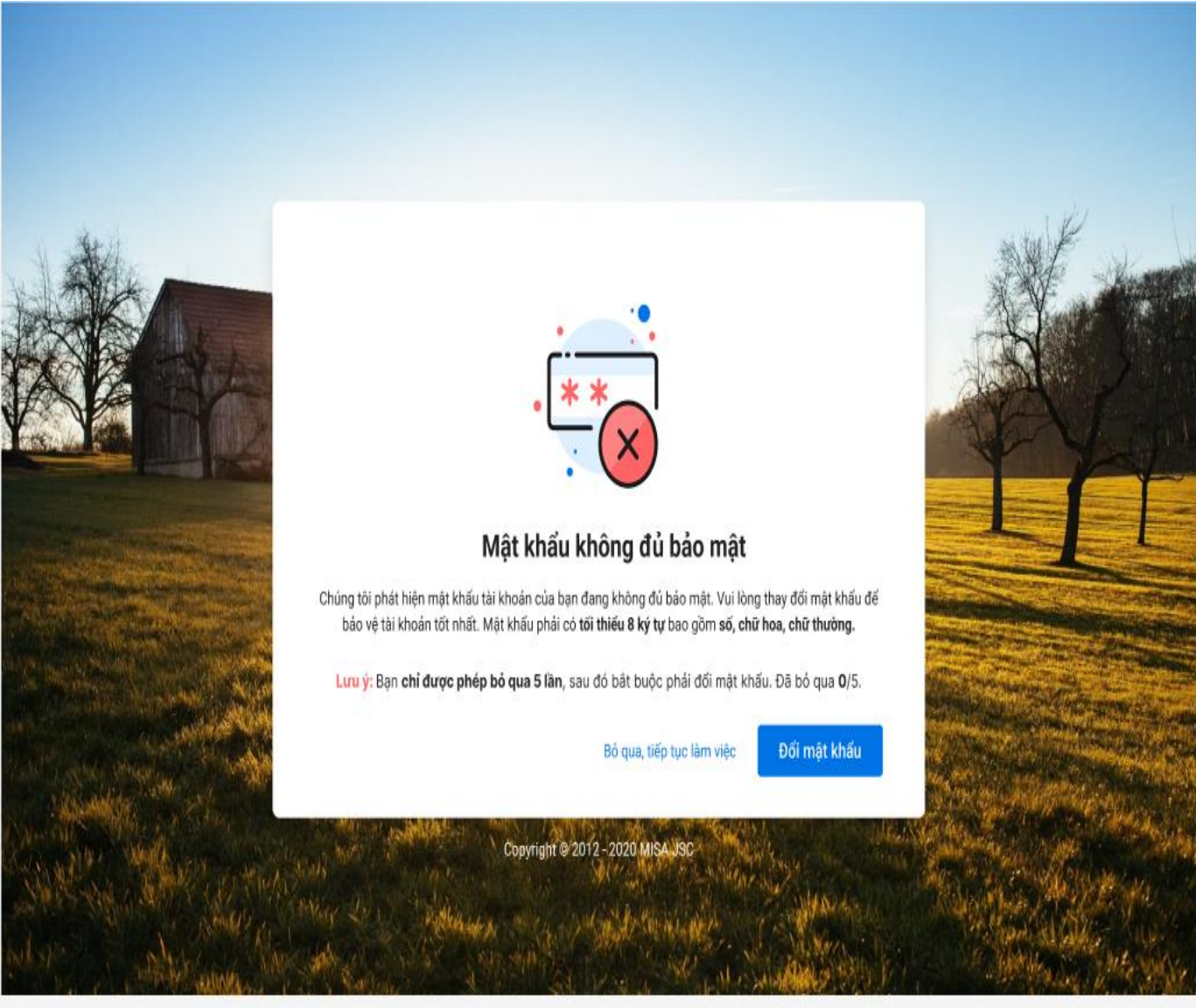
1.1 Điều kiện

Người dùng đăng nhập thành công vào hệ thống với tài khoản có quyền. Hệ thống hiển thị yêu cầu/kiến nghị đổi mật khẩu với các user dung pass yếu.

1.2 Mô tả quy trình nghiệp vụ



Người dùng đăng nhập thành công vào hệ thống, hệ thống kiểm tra chất lượng mật khẩu của người dùng Đối với người dùng đặt mật khẩu không đủ bảo mật, hệ thống thông báo theo màn hình trên





Người dùng lựa chọn **Tiếp tục sử dụng** hoặc **Đổi mật khẩu**. Đối với trường hợp người dùng chọn **Đổi mật khẩu**, hệ thống đưa ra màn hình thiết lập mật khẩu mới

Hệ thống kiểm tra độ mạnh của mật khẩu

Thiết lập mật khẩu để bắt đầu làm việc

Mật khẩu phải có tối thiểu 8 ký tự bao gồm số, chữ hoa, chữ thường.

Mật khẩu hiện tại \*\*\*\*\*

Mật khẩu mới \*\*\*\*\*

X Có ít nhất 8 ký tự

X Có chữ thường (a-z) và chữ in hoa (A-Z)

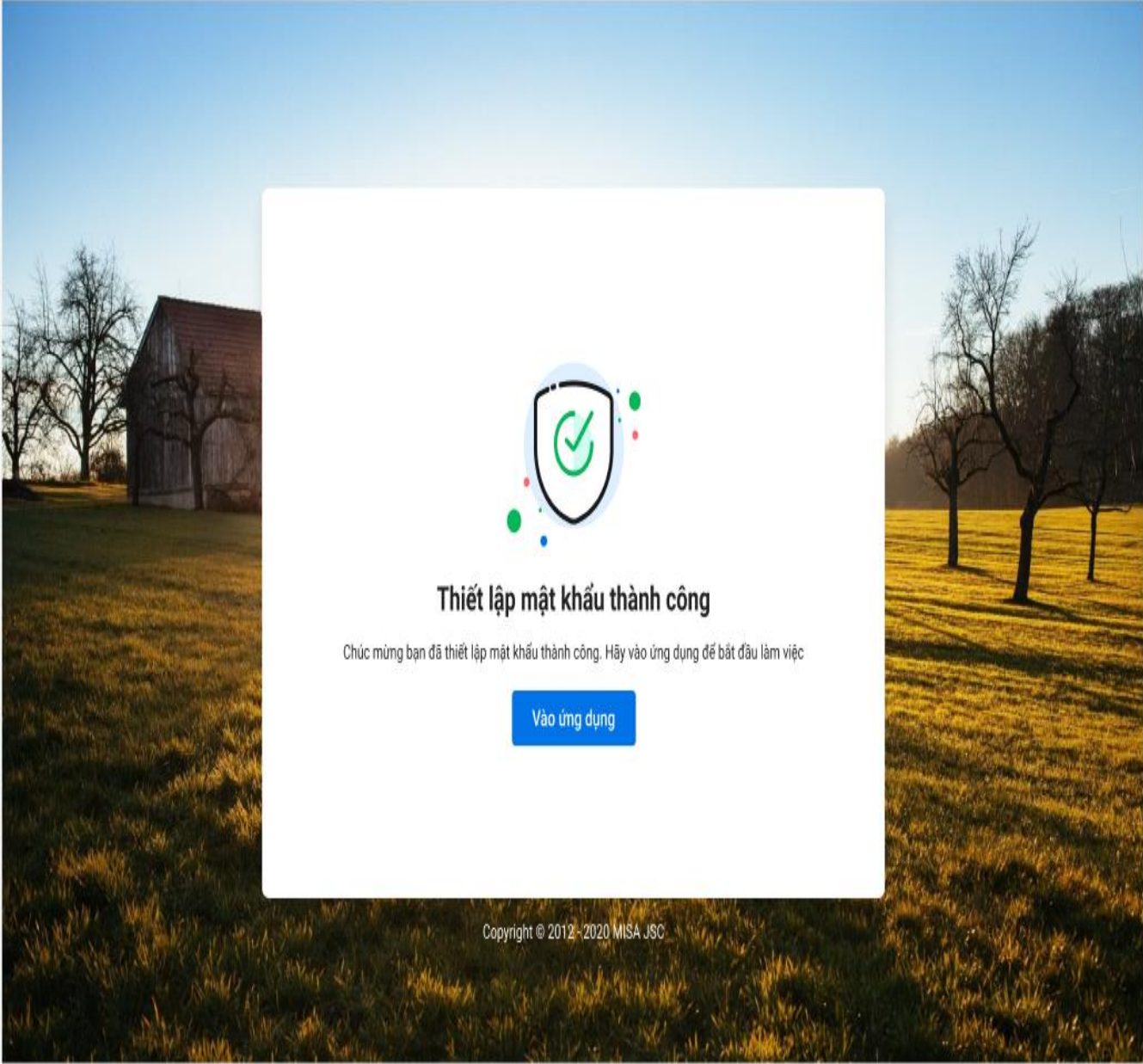
✓ Có ít nhất một chữ số (0-9)

Xác nhận mật khẩu mới

Đặt mật khẩu

Copyright © 2012 - 2020 MISA JSC

Người dùng thiết lập mật khẩu thành công, hệ thống đưa ra thông báo **Thiết lập mật khẩu thành công** và đưa ra lựa chọn **Vào ứng dụng**



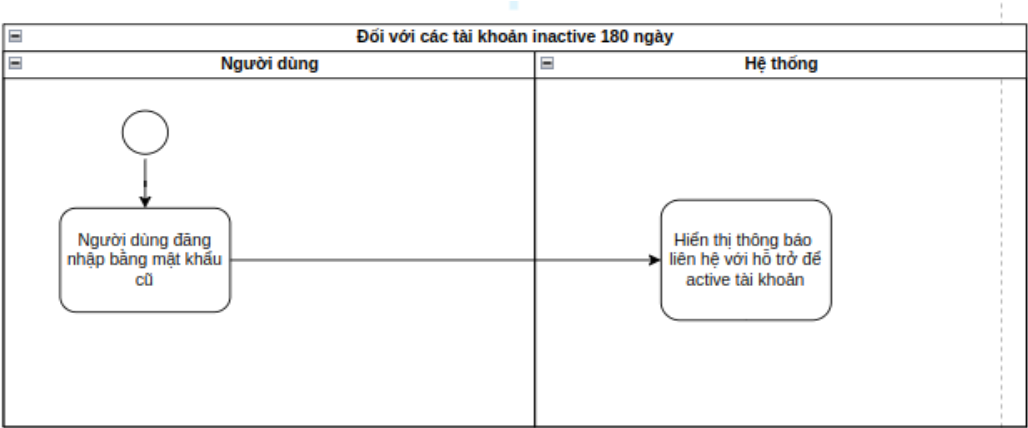
III.ĐẶC TẢ CHI TIẾT CHỨC NĂNG

2. Đối với các user dùng pass yếu, quá [180] ngày chưa có login thì inactive, sau khi đc active lại thì login xong yêu cầu đổi pass (Chỉ áp dụng đối với các App khối Hành chính sự nghiệp)

2.1 Điều kiện

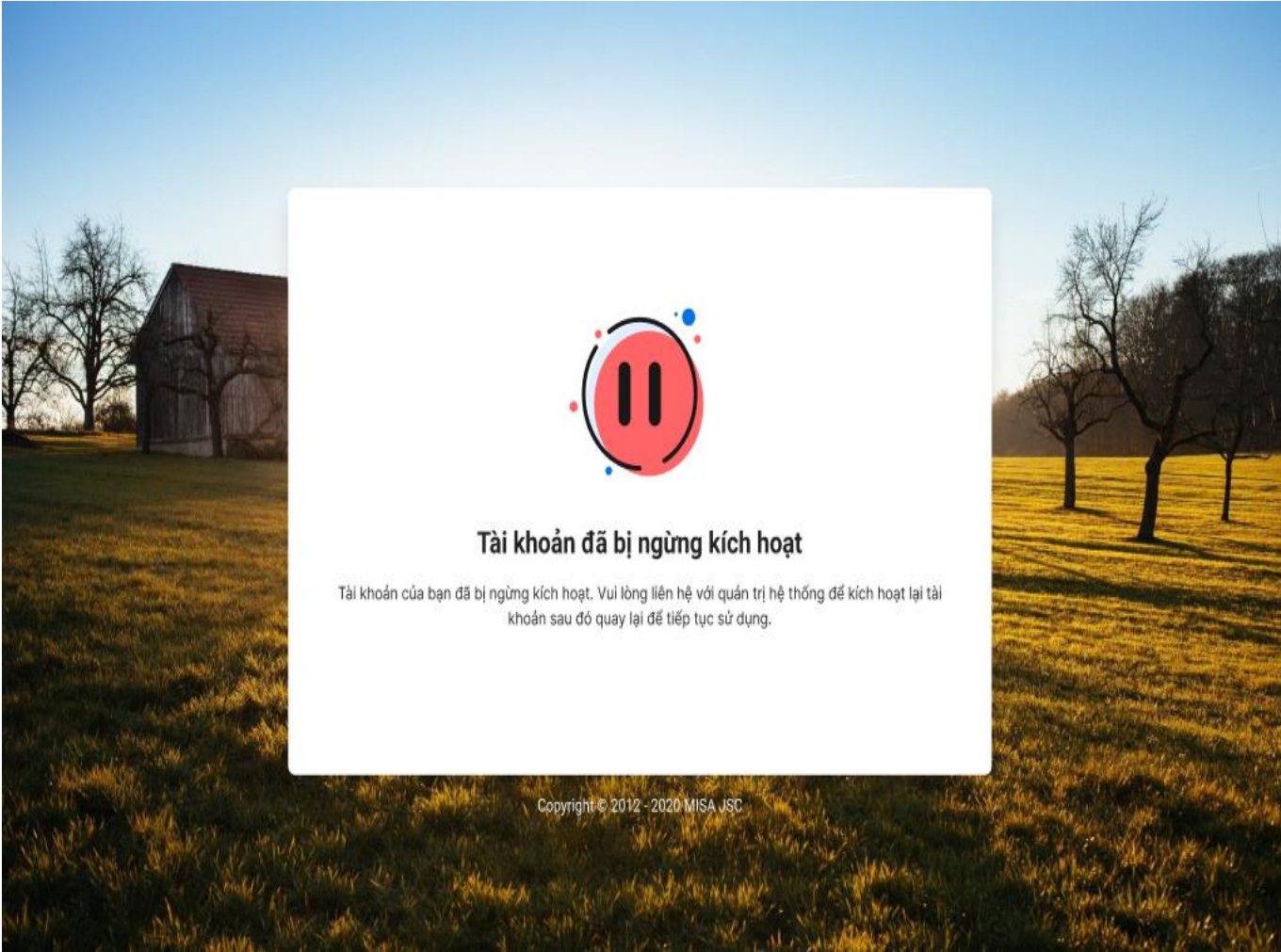
- a.Người dùng đăng nhập vào tài khoản thành công đối với tài khoản bị inactive, sau khi đăng nhập hệ thống hiển thị thông báo liên hệ với quản trị hệ thống để active lại tài khoản
- b.Sau khi active lại tài khoản, hệ thống đưa ra khuyến nghị đổi mật khẩu theo luồng "Đối với người dùng đang sử dụng mật khẩu không đủ bảo mật, sau khi đăng nhập vào xong phần mềm cần yêu cầu/khuyến nghị đổi pass"

2.2 Mô tả quy trình nghiệp vụ





Người dùng đăng nhập thành công vào hệ thống thành công, hệ thống thông báo "Tài khoản đã bị ngừng kích hoạt" và yêu cầu liên hệ để active lại tài khoản



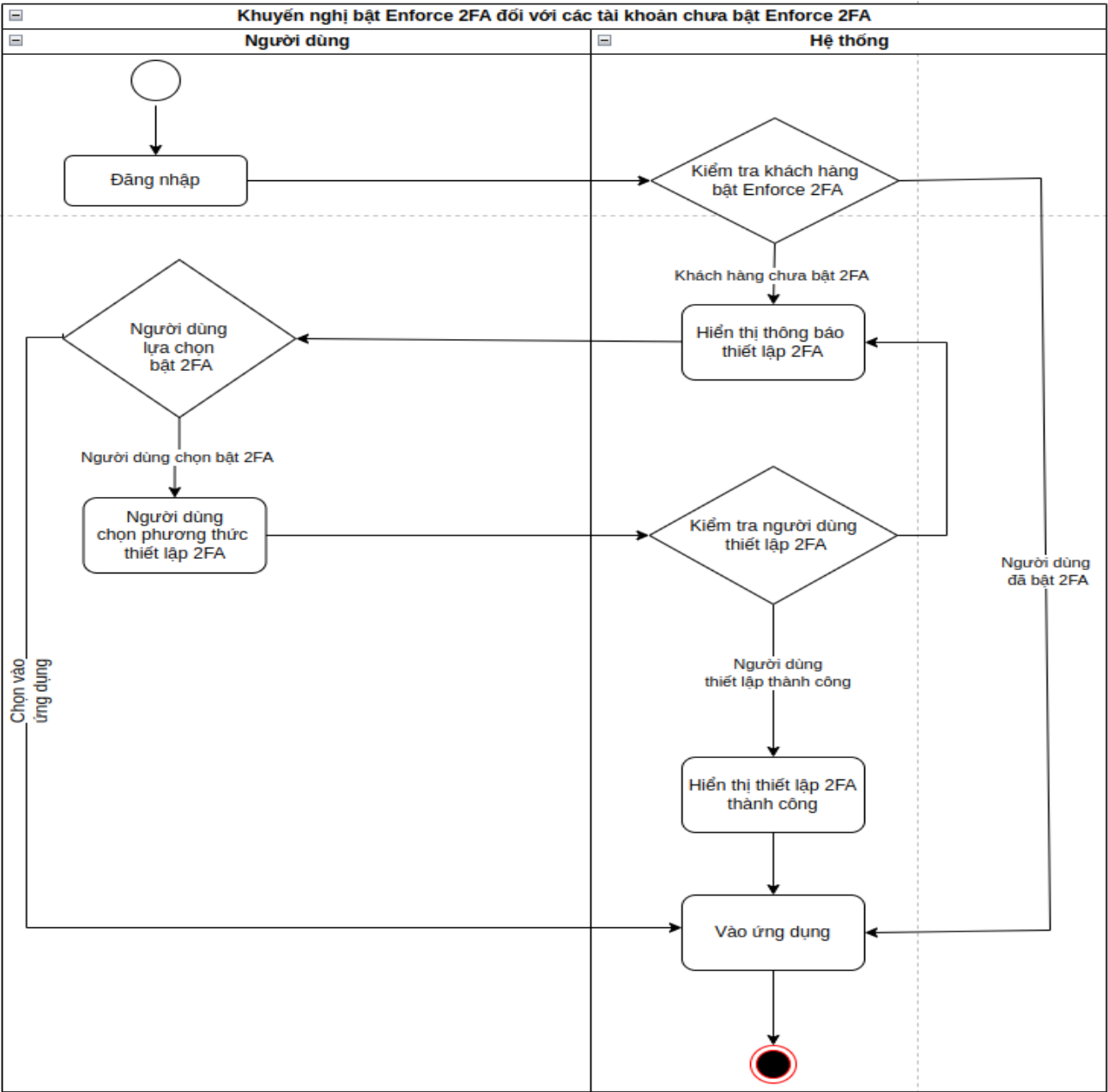
III.ĐẶC TẢ CHI TIẾT CHỨC NĂNG

3. Đối với các user chưa đặt 2FA thì sau khi login xong phần mềm khuyến nghị bật 2FA

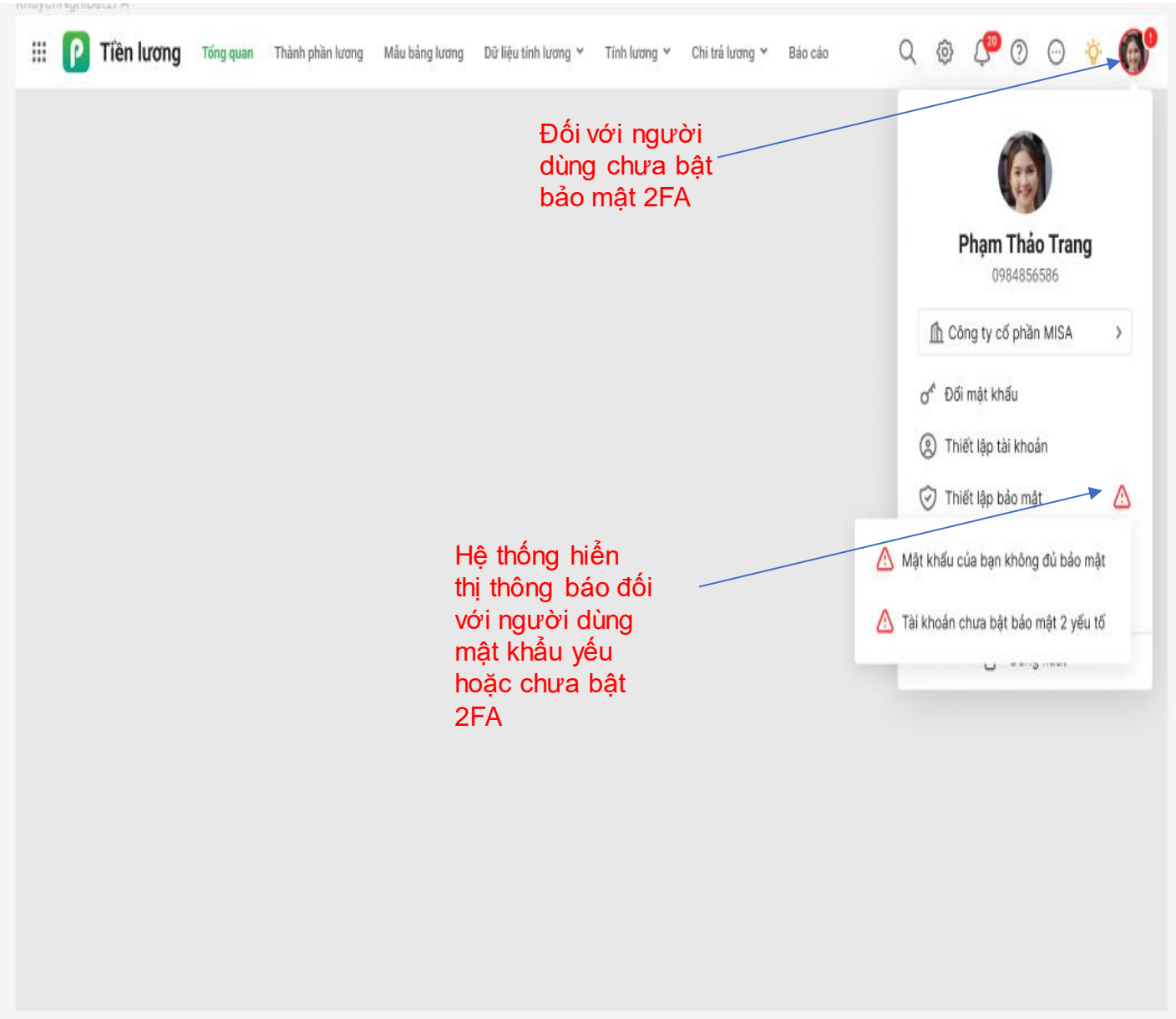
3.1 Điều kiện

Người dùng đăng nhập thành công vào hệ thống với tài khoản có quyền. Hệ thống hiển thị yêu cầu/khuyến nghị thiết lập bảo mật 2 lớp **Enforce 2FA**

3.2.Mô tả quy trình nghiệp vụ



Người dùng đăng nhập thành công vào hệ thống, hệ thống kiểm tra trạng thái thiết lập bảo vệ 2 lớp Enforce 2FA. Nếu chưa thiết lập thì hệ thống đưa ra yêu cầu/khuyến nghị bảo mật trên thông báo tài khoản của người người dùng



Khách hàng chọn **Bật bảo mật 2 yếu tố**, hệ thống hiển thị màn hình thiết lập bảo mật

- Thông tin cá nhân
- Bảo vệ tài khoản**
  - Thông tin đăng nhập
  - Thiết bị đã đăng nhập
  - Nhật ký hoạt động
  - Ứng dụng liên kết
  - Tài khoản liên kết
  - Xóa tài khoản
- Chính sách quyền riêng tư
- Giấy phép & Thanh toán
- Giới thiệu - Tích điểm

← Xác thực 2 yếu tố



**Bảo vệ tài khoản của bạn bằng Xác thực 2 yếu tố**

Nếu phát hiện thấy lần đăng nhập từ thiết bị hoặc trình duyệt lạ, chúng tôi sẽ yêu cầu bạn cung cấp mật khẩu và mã xác thực

Bắt đầu thiết lập

III.ĐẶC TẢ CHI TIẾT CHỨC NĂNG

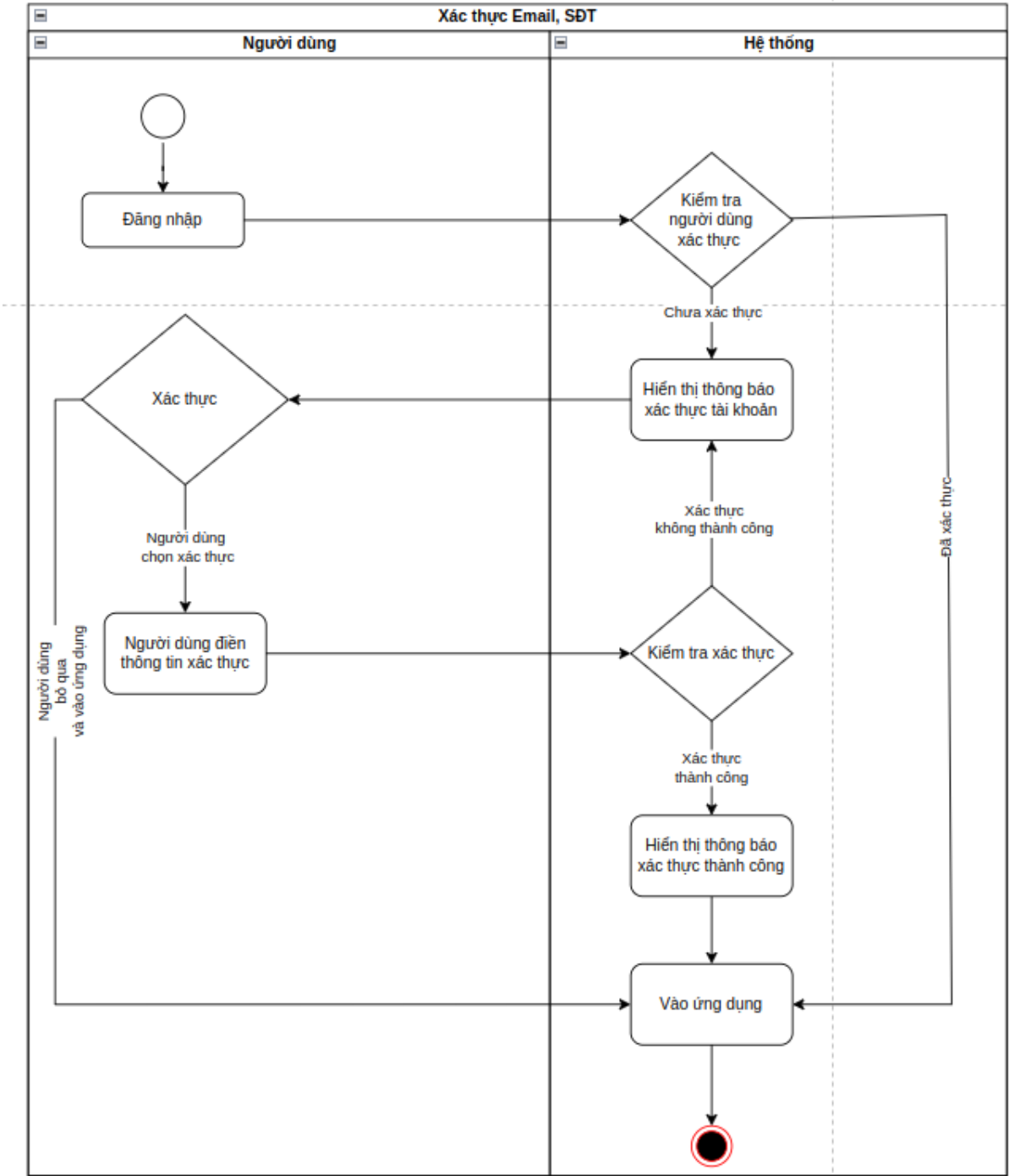
4. Đối với các user chưa verify thông tin, sau khi login xong phần mềm yêu cầu verify (Email, Mobile) để sau này có thể tự lấy lại pass

4.1 Điều kiện


Người dùng đăng nhập thành công vào hệ thống với tài khoản có quyền. Hệ thống hiển thị yêu cầu/kiến nghị xác thực tài khoản qua email

4.2.Mô tả quy trình nghiệp vụ

- Đối với người dùng HCSN trong các giai đoạn tập huấn/ dùng thử
  - + Các tài khoản đã có Emai/SĐT nhưng chưa được xác thực
  - + Các tài khoản chưa có email và SĐT và chưa xác thực
  - + Các tài khoản đã có Email/SĐT cần thay đổi xác thực







### Xác thực tài khoản


Tài khoản của bạn chưa xác thực. Vui lòng **nhập chính xác email để xác thực tài khoản**. Khi tài khoản được xác thực bạn sẽ dễ dàng lấy lại mật khẩu, nhận các thông báo thay đổi của hệ thống kịp thời.

Email

☐ Xác thực bằng số điện thoại ☐ Bỏ qua, tiếp tục làm việc

Copyright © 2012 - 2020 MISA JSC

Màn hình xác thực bằng Email:  
Hệ thống sẽ hiển thị Email mặc định khi  
đăng ký Tài khoản



### Xác thực tài khoản

Tài khoản của bạn chưa xác thực. Vui lòng **nhập chính xác số điện thoại để xác thực tài khoản**. Khi tài khoản được xác thực bạn sẽ dễ dàng lấy lại mật khẩu, nhận các thông báo thay đổi của hệ thống kịp thời.

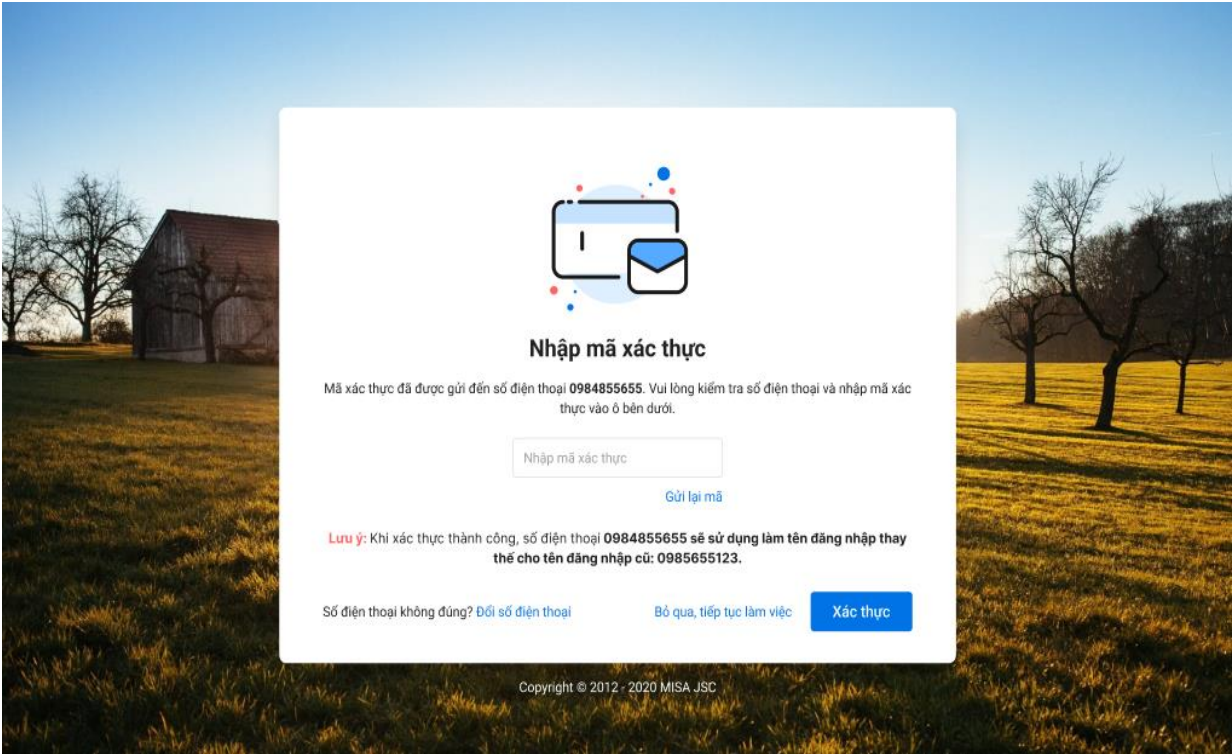
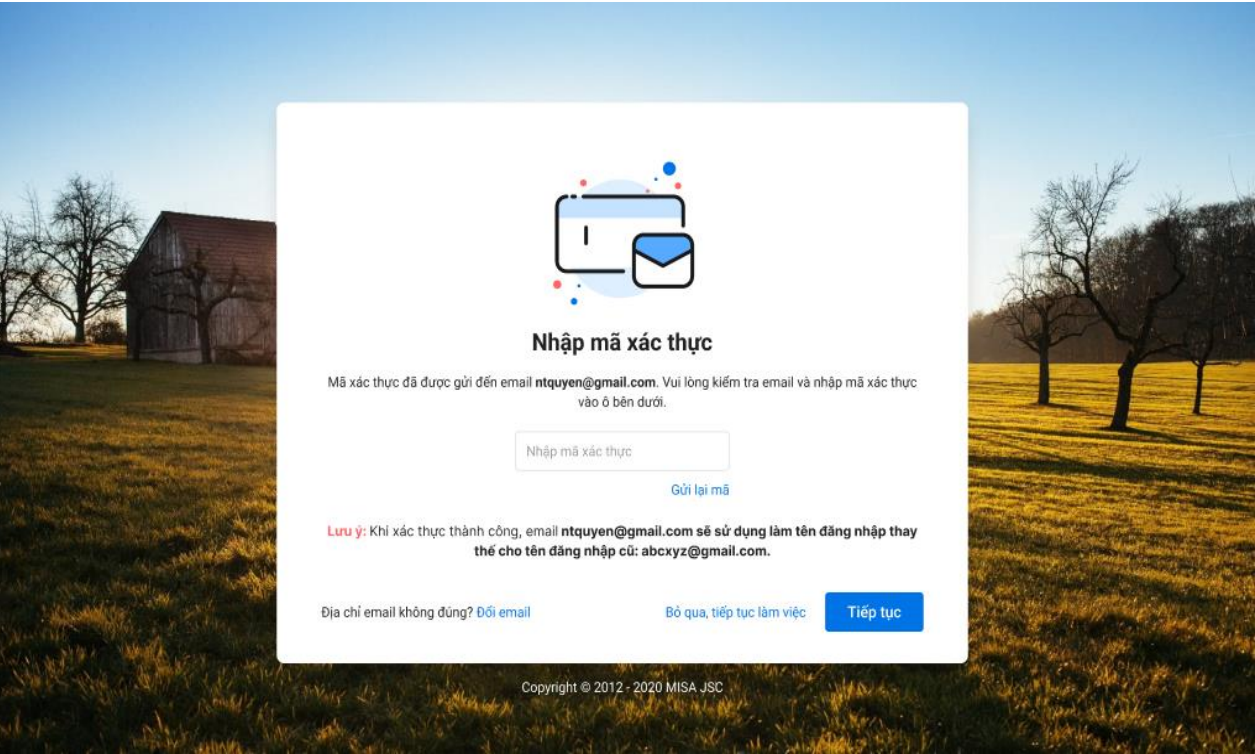
Số điện thoại

☒ Xác thực bằng email ☐ Bỏ qua, tiếp tục làm việc

Copyright © 2012 - 2020 MISA JSC

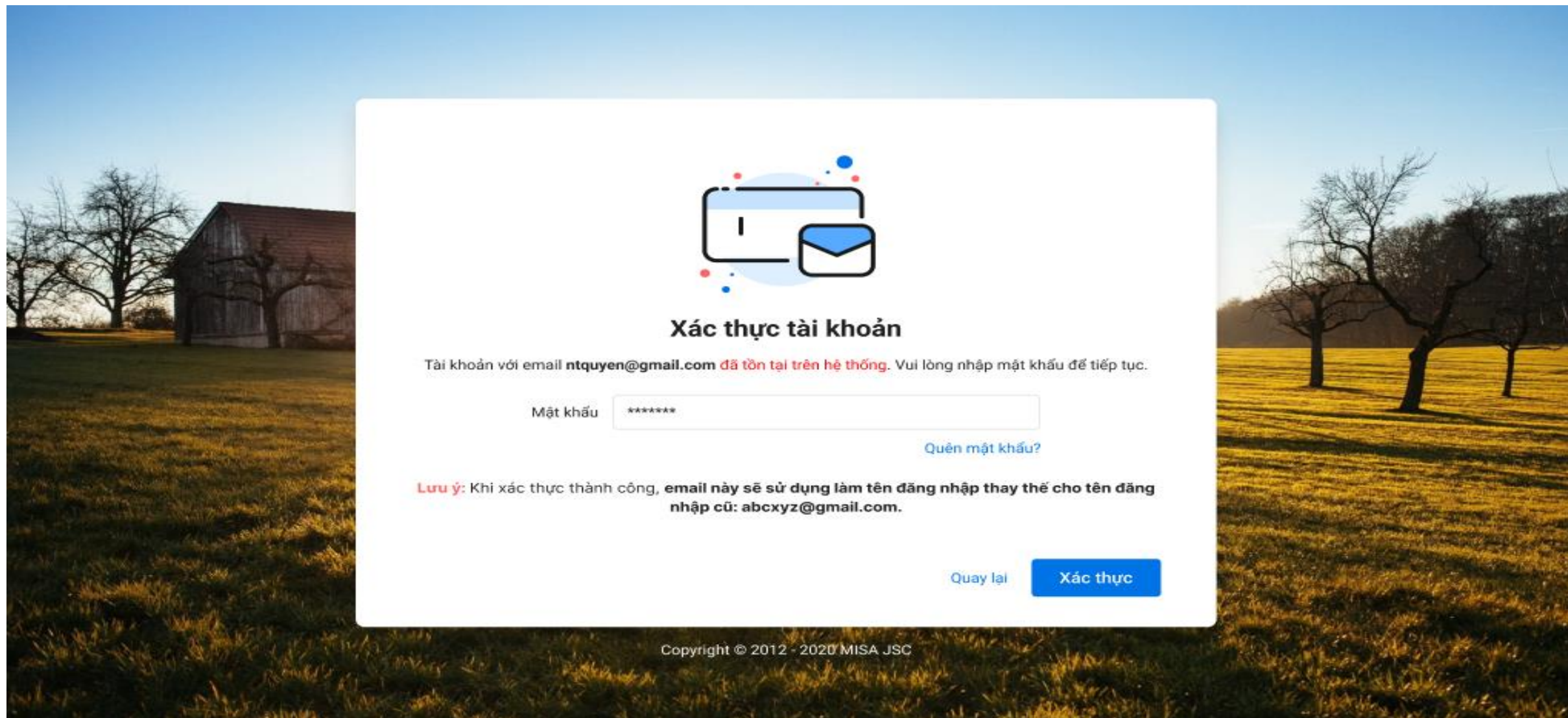
Màn hình xác thực bằng Số điện thoại:  
Hệ thống sẽ hiển thị SĐT mặc định khi đăng  
ký Tài khoản


Người dùng lựa chọn **Bỏ qua**, **Tiếp tục làm việc** hoặc **Tiếp tục**. Đối với trường hợp người dùng chọn **Tiếp tục**, hệ thống đưa ra màn hình





Thông báo sẽ hiển thị Email/SĐT thay thế cho Email/SĐT cũ, đối với Email/SĐT đã tồn tại trên hệ thống, hệ thống sẽ hiển thị





## Xác thực tài khoản

Tài khoản với email **ntquyen@gmail.com** đã tồn tại trên hệ thống. Vui lòng nhập mật khẩu để tiếp tục.

Mật khẩu

\*\*\*\*\*

[Quên mật khẩu?](#)

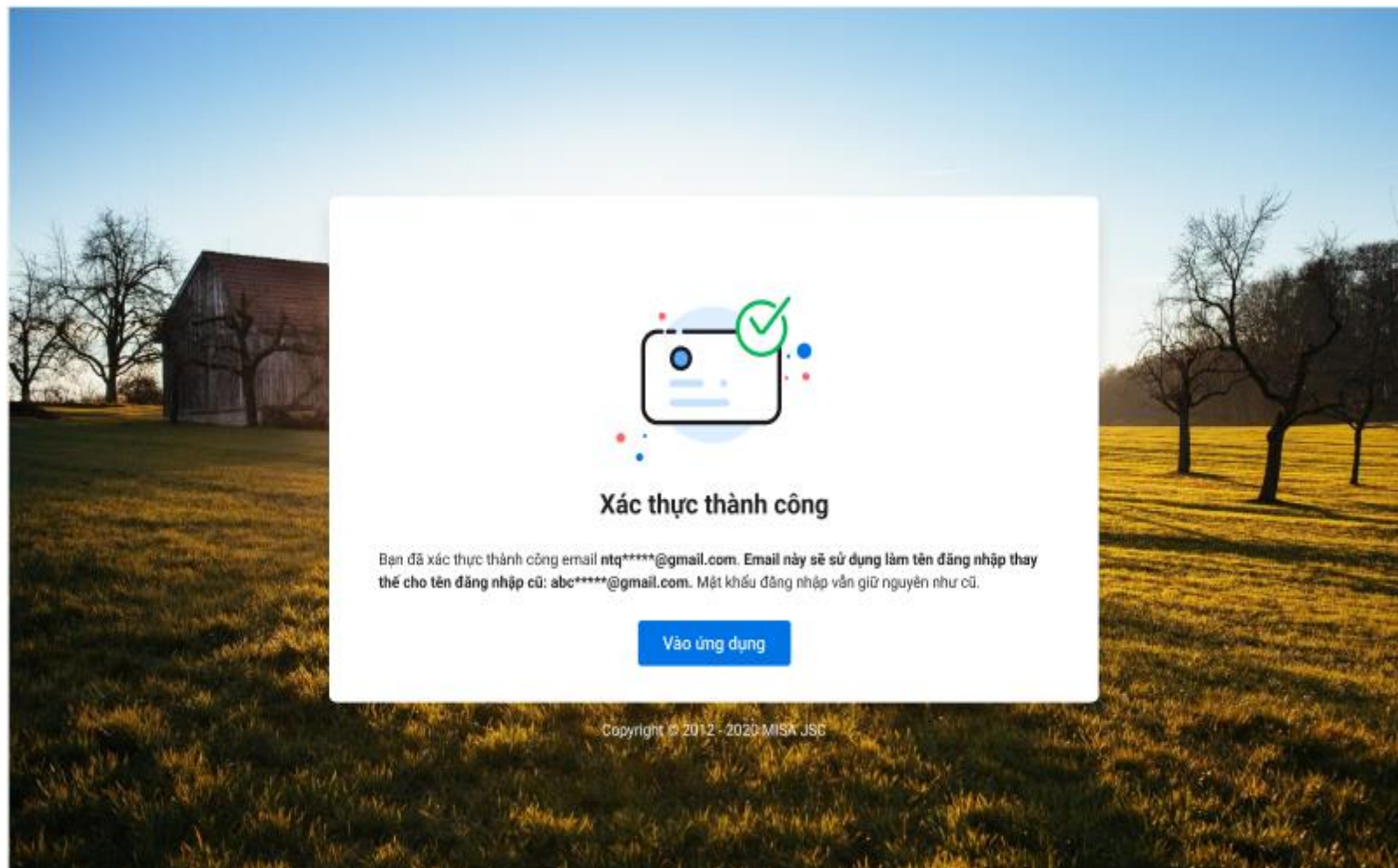
**Lưu ý:** Khi xác thực thành công, email này sẽ sử dụng làm tên đăng nhập thay thế cho tên đăng nhập cũ: **abcxyz@gmail.com**.

[Quay lại](#)

[Xác thực](#)

Copyright © 2012 - 2020 MISA JSC

Thông báo hiển thị khi người dùng xác thực thành công.



### III.ĐẶC TẢ CHI TIẾT CHỨC NĂNG

**5. Đối với trường hợp Admin bật bảo mật 2 lớp 2FA cho tất cả các người dùng**

**5.1 Điều kiện**

Admin bật yêu cầu bảo mật 2 lớp 2FA cho tất cả các user

**5.2.Mô tả quy trình nghiệp vụ**



Admin bật xác thực 2 yếu tố (2FA) cho tất cả người dùng

System

Thông tin công ty

Ứng dụng

Người dùng

Nhóm

Quản trị hệ thống

Cấu hình mail server

**Bảo mật nâng cao**

Nhật ký hoạt động

Thùng rác

Bảo mật nâng cao

Hủy

Lưu

TỰ ĐỘNG ĐĂNG XUẤT

☐

Tự động đăng xuất

Tính từ thời điểm người dùng đăng nhập, cứ sau khoảng thời gian đã thiết lập hệ thống sẽ tự động đăng xuất.

XÁC THỰC 2 YẾU TỐ (2FA)

☒ Bắt buộc xác thực 2 yếu tố khi đăng nhập

Khi nhân viên đăng nhập phần mềm sẽ yêu cầu thiết lập 2 yếu tố nếu chưa bật.

☒ Tất cả người dùng

☐ Chỉ người dùng được chọn

GIỚI HẠN TRUY CẬP

☐ Giới hạn truy cập theo địa chỉ IP

Thiết lập các địa chỉ IP được phép truy cập vào hệ thống MISA AMIS của công ty bạn

☐ Giới hạn truy cập theo thời gian

Thiết lập khoảng thời gian cho phép truy cập vào hệ thống MISA AMIS của công ty bạn

Áp dụng giới hạn truy cập cho

☒ Tất cả ứng dụng

☐ Chỉ những ứng dụng được chọn

Danh sách người dùng không bị giới hạn

+ Thêm người dùng

+ Thêm danh sách quản trị

Tìm kiếm

Họ và tên	Email tài khoản	Đơn vị công tác
Không có dữ liệu		

**MISA®**  
TIN CÂY - TIỆN ÍCH - TẬN TÌNH

KHÁCH THÍCH - KHÁCH YÊU - KHÁCH CHIA SẺ

## Trường hợp khách hàng sử dụng phương thức xác thực mặc định


### Thiết lập bảo mật 2 yếu tố (2FA)


Xin chào Hoàng Trung Kiên,

Công ty của bạn đang yêu cầu bạn bật xác thực 2 yếu tố nhằm nâng cao bảo mật. Vui lòng thực hiện theo các bước sau:

[Xem video hướng dẫn](#)

**Bước 1:** Cài đặt ứng dụng xác thực Google Authenticator từ [App Store \(iOS\)](#) hoặc [CH Play \(Android\)](#)

**Bước 2:** Mở ứng dụng và bấm  chọn Quét mã QR để sinh mã xác thực



[Không quét được mã này?](#)

**Bước 3:** Nhập mã xác thực gồm 6 chữ số để sinh ở bước trước:

[Thiết lập bằng phương thức khác](#) [Bỏ qua và Đăng xuất](#) [Tiếp tục](#)

Đối với người dùng không quét được mã, hệ thống sẽ hiển thị


### Thiết lập bảo mật 2 yếu tố (2FA)


Xin chào Hoàng Trung Kiên,

Công ty của bạn đang yêu cầu bạn bật xác thực 2 yếu tố nhằm nâng cao bảo mật. Vui lòng thực hiện theo các bước sau:

[Xem video hướng dẫn](#)


**Bước 1:** Cài đặt ứng dụng xác thực Google Authenticator từ [App Store \(iOS\)](#) hoặc [CH Play \(Android\)](#)

**Bước 2:** Mở ứng dụng và bấm  chọn Quét mã QR để sinh mã xác thực



[Không quét được mã này?](#)

Mở ứng dụng và bấm chọn **Nhập khóa** thiết lập tiếp theo nhập tên tài khoản và mã bên dưới sau đó nhấn **Thêm**

Khóa thiết lập: DOLT T2W3 VYIA FNR7 4ZK5 YYKX J37U 533B 

**Bước 3:** Nhập mã xác thực gồm 6 chữ số để sinh ở bước trước:

[Thiết lập bằng phương thức khác](#) [Bỏ qua và Đăng xuất](#) [Tiếp tục](#)



## Trường hợp khách hàng sử dụng phương thức xác thực khác

Thiết lập bằng phương thức khác

Nhận mã xác thực qua số điện thoại \*\*\*\*\*565

Nhận mã xác thực qua Email he\*\*\*\*\*abc@gmail.com

Nhận mã xác thực từ ứng dụng Google Authenticator

Bỏ qua và Đăng xuất

Copyright © 2012 - 2020 MISA JSC

Thiết lập bảo mật 2 yếu tố (2FA)

Nhập mã xác thực

Mã xác thực đã được gửi về email he\*\*\*\*\*abc@gmail.com. Bạn vui lòng kiểm tra email và nhập chính xác mã vào ô dưới để hoàn tất quá trình thiết lập

Nhập mã xác thực

Gửi lại mã

Thiết lập bằng phương thức khác

Bỏ qua và Đăng xuất

Tiếp tục

Copyright © 2012 - 2020 MISA JSC

**MISA**<sup>®</sup>  
TIN CÂY - TIỆN ÍCH - TẬN TÌNH

**KHÁCH THÍCH - KHÁCH YÊU - KHÁCH CHIA SẺ**



## Bật bảo mật 2 yếu tố (2FA) thành công

Bạn đã bật thành công bảo mật 2 yếu tố bằng hình thức sinh mã xác thực qua ứng dụng **Google Authenticator**.

Để sử dụng thêm các phương thức xác thực khác như: **Xác thực qua email**, **Xác thực qua số điện thoại** vui lòng thiết lập [tại đây](#).

Vào ứng dụng

Copyright © 2012 - 2020 MISA JSC