

CÔNG TY CỔ PHẦN CÔNG NGHỆ PIHOME

Địa chỉ: 637/37/37 Quang Trung, Phường 11, Quận Gò Vấp, TP.HCM

MST: 0315917583

Website: www.pihome.asia

BẢO MẬT VÀ QUYỀN RIÊNG TƯ

(PIHOME' S STATEMENT OF SECURITY AND PRIVACY)

TP.HCM. ngày 02 tháng 01 năm 2023

1. Tiêu chuẩn Bảo mật và Quyền riêng tư

Bảo vệ dữ liệu của khách hàng là ưu tiên hàng đầu tại PiHome. Nguyên tắc cơ bản này giúp thiết lập niềm tin với khách hàng và PiHome có sẵn các bộ tiêu chuẩn cao trong ngành để bảo vệ niềm tin đó. Khách hàng và người dùng của chúng tôi có quyền kiểm soát và quyền sở hữu đối với dữ liệu của họ. PiHome áp dụng cách tiếp cận toàn diện để xây dựng một hệ thống phòng thủ kết hợp các hoạt động và dịch vụ bảo mật chất lượng hàng đầu, đồng thời cung cấp các tính năng và giải pháp tuân thủ bảo mật toàn diện để giúp quản trị viên doanh nghiệp tạo dựng niềm tin với các thành viên và đáp ứng các yêu cầu tuân thủ dữ liệu toàn cầu.

1.1 Tiêu chuẩn bảo mật

- **Máy chủ & Lưu trữ dữ liệu (Server & Data Storage):** Phần mềm PiHome được triển khai song song trên hạ tầng đám mây của Amazon AWS và Microsoft Azure, dựa vào khả năng bảo mật hàng đầu của AWS và Azure để đảm bảo an toàn cho cơ sở hạ tầng của toàn bộ hệ thống PiHome. Sử dụng kiến trúc bảo mật đám mây hàng đầu trên với khả năng phát hiện cơ bản, quét lỗ hổng, phát hiện xâm nhập, bảo mật vùng chứa (container), cách ly dịch vụ và cơ chế truy cập không tin cậy để luôn bảo mật hoạt động kinh doanh của PiHome. Việc triển khai song song trên hai hạ tầng hàng đầu thế giới giúp hạn chế tối đa các rủi ro có thể xảy ra, bao gồm các kịch bản chống thảm họa. Các cuộc diễn tập khắc phục thảm họa và kiểm tra khôi phục dữ liệu thường xuyên được tiến hành để đảm bảo hoạt động kinh doanh liên tục trong trường hợp xảy ra bất kỳ thảm họa hoặc sự cố lớn bất ngờ nào. Ngoài ra, để đáp ứng về tiêu chuẩn lưu trữ dữ liệu tại Việt Nam theo nghị định 13/2023/NĐ-CP của Chính phủ, PiHome trang bị thêm hạ tầng đồng bộ hoá dữ liệu nhằm đảm bảo cơ sở dữ liệu cư dân luôn được lưu trữ tại Việt Nam.
- **Quyền truy cập dữ liệu (Data Access):** PiHome có sẵn các giao thức nghiêm ngặt để đảm bảo rằng quyền truy cập vào dữ liệu người dùng được kiểm soát và cách ly. Nếu không có sự cho phép thích hợp, người dùng không thể truy cập dữ liệu của nhau và mọi quyền truy cập vào dữ liệu phải được chủ sở hữu dữ liệu cho phép rõ ràng. Theo mặc định, nhân viên của chúng tôi không có quyền truy cập vào bất kỳ dữ liệu người dùng nào. Trong quá trình triển khai và hỗ trợ sau triển khai, các dữ liệu nhạy cảm (sensitive data) của khách hàng nhân sự của PiHome không chủ động thao tác trực tiếp trên dữ liệu mà chỉ hướng dẫn, đào tạo để nhân sự của khách hàng tự thao tác trên máy của khách hàng. Trường hợp phía khách hàng gửi dữ liệu cho nhân sự PiHome, điều này đồng nghĩa với việc PiHome có quyền miễn trừ trách nhiệm trong trường hợp đó.
- **Bảo mật dữ liệu (Data Security):** PiHome áp dụng các biện pháp tổ chức và bảo mật nghiêm ngặt ở mọi giai đoạn thu thập, truyền và lưu trữ dữ liệu. Chúng tôi sử dụng nhiều phương pháp mã hóa và giám sát quy trình khác nhau để phát hiện và giải quyết các bất thường càng sớm càng tốt, đảm bảo tính bảo mật của dữ liệu trong suốt vòng đời của dữ liệu. PiHome cũng mã hoá dữ liệu nhạy cảm ở tầng database nhằm hạn chế rủi ro từ việc hacker truy cập trái phép từ bên ngoài. PiHome có cơ chế quản lý dữ liệu hoàn chỉnh trong vòng đời và có quy trình rõ ràng cũng như đảm bảo kỹ thuật cho việc tạo, lưu trữ, truyền, sử dụng và hủy dữ liệu.

PiHome cũng cung cấp các giải pháp Dịch vụ quản lý khóa (KMS) và Mang theo khóa riêng của bạn (BYOK) để tăng cường bảo vệ bảo mật dữ liệu (Đối với phương án triển khai Hybrid - Data lưu trữ trên server do khách hàng chỉ định).

- **Bảo mật mã nguồn (Source code Security):** Source code được đội ngũ PiHome tự phát triển, đã được đăng ký bảo hộ bản quyền tác giả, dựa trên kiến trúc microservices, các service hoạt động độc lập nhau kể cả source code, database và service này không thao tác được đến database của services khác. Trong từng service, database không nằm chung với api server. Mỗi database trên một service chỉ có server ở service đó mới kết nối tới được. Mọi truy cập từ bên ngoài chỉ thông qua api gateway. Các services giao tiếp với nhau thông qua private network. Lập trình viên theo đó chỉ được kết nối thông qua SSH Key và VPN. Tại API Gateway sử dụng tường lửa WAF (Web Application Firewall) của AWS và cloudfront, route53. API bao gồm cụm với các api gateway nhỏ, áp dụng kỹ thuật load balancer để điều phối lượng API nhằm tránh tình trạng bị tấn công từ chối dịch vụ (DDoS). Quy trình xác thực truy cập thông qua đăng nhập với nhiều phương pháp, hệ thống tự động phát hiện và chặn các thao tác “dò tìm password” phổ biến và gửi cảnh báo đến security team khi có phát hiện bất thường. Ngoài ra, source code được minify và uglify code để tránh bị đọc mã nguồn sai phép, source được gom chung để nén và sau đó chia nhỏ ra để tải nhằm che giấu source code tốt hơn từ bên ngoài. Các giao tiếp trên source đều thông qua https protocol, sử dụng passport để giao tiếp và xác thực users.
- **Bảo mật tài khoản (Account Security):** PiHome hỗ trợ Đăng nhập một lần (SSO) thông qua các giao thức chuẩn và nền tảng nhận dạng hiện có của doanh nghiệp, tuân thủ các chính sách và thông số bảo mật tài khoản của doanh nghiệp. PiHome cũng cung cấp tùy chọn sử dụng xác thực của riêng mình để tăng cường bảo mật tài khoản thông qua xác minh hai bước và các tính năng khác.
- **Quyền của thành viên (Member Permission):** PiHome cung cấp các biện pháp kiểm soát quyền linh hoạt để giúp quản trị viên chỉ cấp những quyền cần thiết cho thành viên tổ chức. Thông qua cấu hình hiển thị và quyền liên lạc và cộng tác, quản trị viên có thể tạo ra các rào cản thông tin trong tổ chức để ngăn chặn sự xáo trộn thông tin không hiệu quả đối với những nhân viên nhạy cảm và bảo vệ thông tin nhạy cảm trong tổ chức. Bộ phân quyền của PiHome được phát triển chi tiết cho từng vai trò (role), nhóm quyền, quyền giúp phân quyền cho bất kỳ user nào một cách dễ dàng, chính xác và linh hoạt.
- **An ninh mạng máy tính (Network Security):** Thiết kế các cụm thiết bị mạng, độc lập cách ly với nhau, triển khai đa hoạt động khắc phục sự cố cấp thiết bị; được trang bị một cổng mạnh mẽ và cơ chế kiểm soát truy cập, đồng thời mã hóa nghiêm ngặt tất cả các quy trình truyền thông tin liên lạc để chống lại hành vi xâm nhập và chiếm quyền điều khiển độc hại từ bên ngoài.
- **Bảo mật tầng ứng dụng (Application Security):** Tất cả ứng dụng được phát triển hoặc tích hợp từ bên thứ 3 đều thông qua API và được điều phối đến tầng database tương ứng để trao đổi dữ liệu. Tại tầng ứng dụng, các dữ liệu nhạy cảm được che giấu thông tin (ví dụ: email, số điện thoại) và lưu vết tất cả truy vấn để đọc thông tin này từ người dùng. Dữ liệu nhạy cảm export ra khỏi hệ thống sẽ tự động được mã hóa che giấu nhằm tránh lộ thông tin từ file export.
- **Sao lưu dữ liệu (Data Backup):** Dữ liệu quan trọng được backup thường xuyên hàng ngày và lưu trữ liên tục trong 30 ngày. Source code được backup hàng ngày, đồng bộ trên hai môi trường staging và production.
- **Đảm bảo tính hiệu dụng cao (High Availability):** Hệ thống đảm bảo tính hiệu dụng 99,99% down-time bằng cách sử dụng nhiều kỹ thuật như cân bằng tải (load balancer), EC2 multi AZ, auto scaling ở tầng source và

load balancer, multi AZ, Replica ở tầng database. Sử dụng SNS alert báo về cho System Admin khi bị gián đoạn hoặc quá tải trên service. Elastic load balancer để tự động điều hướng network.

- Về quy trình triển khai (Deployment): Chúng tôi ưu tiên bảo mật ở mọi giai đoạn trong quá trình quản lý vòng đời phát triển sản phẩm (*Dev - Staging - Production*) để đảm bảo dịch vụ ổn định, tránh gián đoạn và an toàn cho người dùng. Bộ phận DevOps của chúng tôi được hỗ trợ bởi đội ngũ vận hành bảo mật chuyên nghiệp và các cơ chế vận hành bảo mật tiêu chuẩn cao để giải quyết kịp thời các sự cố bảo mật và ứng phó ngay khi chúng tôi phát hiện ra.

Các lập trình viên PiHome không được quyền truy cập trực tiếp vào server production ngoại trừ nhân sự cốt lõi được cấp phép đặc biệt từ Ban lãnh đạo công ty. Khi sự cố xảy ra, dữ liệu debug được trích xuất dưới dạng mã, lập trình viên không thể giải mã nếu không có key trực tiếp từ production. Dữ liệu cho lập trình viên debug được duyệt bởi cấp cao (CTO/ BOD).

Quy trình triển khai mã nguồn CI/CD được tự động hoá hoàn toàn thông qua CodePipeline, CodeBuild và Kubernetes (K8s).

1.2 Quyền riêng tư

- Dữ liệu của bạn nằm trong tầm kiểm soát của bạn là triết lý của PiHome. Khách hàng và người dùng có quyền kiểm soát cách xử lý dữ liệu tạo và lưu trong PiHome. Trên hệ thống PiHome, những dữ liệu nào do khách hàng là bên nhập thì khách hàng có quyền huỷ dữ liệu khi không còn hợp tác, những dữ liệu nào là thông tin cá nhân do cư dân tự nhập thì cư dân được quyền huỷ dữ liệu đó trên ứng dụng. Tài khoản ứng dụng di động của cư dân chỉ cư dân đó mới được đăng nhập với password là OTP dùng một lần.
- PiHome được thiết kế để đáp ứng các yêu cầu pháp lý và quy định quốc tế cũng như các tiêu chuẩn ngành quản lý vận hành bất động sản liên quan
- Cởi mở và minh bạch: các vấn đề liên quan đến dữ liệu nhạy cảm và quyền riêng tư được PiHome cam kết giải quyết mọi thắc mắc của khách hàng và cư dân với tinh thần cầu thị, cởi mở và minh bạch, thượng tôn pháp luật.

CÔNG TY CỔ PHẦN CÔNG NGHỆ PIHOME

Giám Đốc



TRẦN BÁ THÌN