ethnio tm

Security Overview

VERSION NO. 5
CREATED AUG 21, 2018

ETHNIO, INC.
6121 W SUNSET BLVD
LOS ANGELES, CA 90028
TEL (888) 879-7439
ETHN.IO

Summary

Since its creation in 2009, Ethnio security procedures and policies have evolved according to industry best practices. We understand that placing third-party code on your web site or in your native iOS/ Android app can involve security approval, and this document is intended to help you cover basic issues with getting Ethnio code approved and placed.

The Basics

Ethnio current runs RubyOnRails 4.2.5 on Ruby 2.3 on Nginx and Unicorn with PostgreSQL and Redis. We've used AngularJS for some navigation, editing questions, scheduling and recruits pages. We use Rails caching based on Redis to show screeners and on marketing pages.

We will not use information gathered from you or Ethnio recruiting screeners in any way, except as described when you agreed to provide it. Furthermore, any other data or information you provide us (including images, email addresses, etc.) will otherwise be held securely. We will never share your information with third parties for marketing purposes, and don't engage in cross-marketing or link-referral programs with other sites. If you have opted-in, we will send you updates and information on Ethnio occasionally, but you can always unsubscribe.

Legal Overview

Ethnio, Inc. — California S-Corp incorporated in 2011. CEO is Nate Bolt.

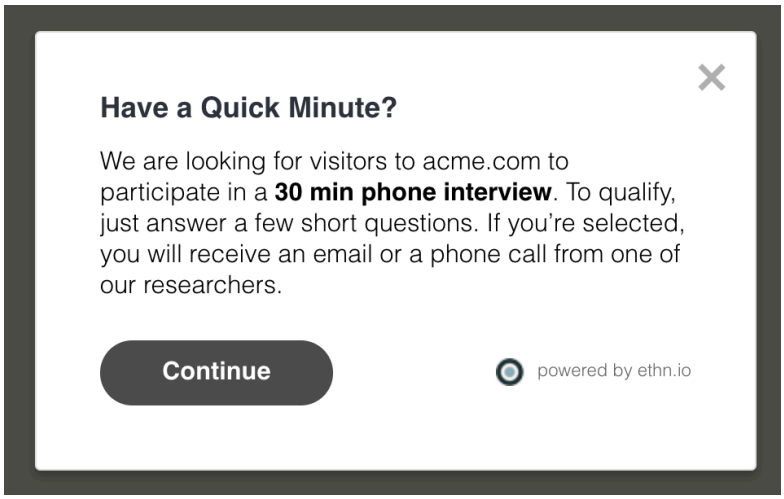
Location: 6121 W Sunset Blvd, Los Angeles, CA 90028

Insurance: $1M umbrella liability by The Hartford

Staff is three developers and one designer, plus contractors.

Primary data center is located at 3000 Irving Blvd., Dallas TX

Data in Recruiting Screeners



Ethnio is a hosted usability service that allows our customers to create recruiting screeners, similar to web surveys. Our customers use our service to post Recruiting Screeners on a website, or send links to those screeners via email or other methods. We have no control over how Ethnio customers use the personal data submitted by users to their recruiting screeners, except if they violate the Ethnio Customer Terms & Conditions, which state that they should only be using recruiting screeners for purposed related to usability or ethnographic research.

If you suspect someone has violated these terms, please contact us. Screener Respondents may have any relationship to our customers, and Ethnio only acts as a Data Processor (a company that processes Personally Identifiable Information on behalf of a Data Controller) so that each Ethnio Customer acts as a Data Controller (a company that determines the purposes for which and the means by which the Personally Identifiable Information is processed).

To process information means to carry out an operation or set of operations on the information, such as collecting, recording, storing, disclosing, or organizing it. Information that Screener Respondents provide to Ethnio Customers passes through our service and resides on our servers, in the most secure manner adhering to industry guidelines. That information may be stored and processed in the United States or any other country in which Ethnio or its affiliates, subsidiaries or agents maintain facilities. The full list of privacy terms can be found here: ethn.io/privacy

Physical Security

The data center runs a Cisco networking environment. and is staffed 24x7 by technicians who perform all our remote work (e.g. changing drives, memory or swapping servers). It's a SAS 70 Type II audited facility in a single-story, single-tenant building for enhanced control and security.

- Multiple layers of security & authentication; including card key, PIN, & biometric required for facility entrance
- Intrusion detection systems to prevent unauthorized electronic access
- Firewall management and monitoring services
- Full CCTV surveillance backed by digital recording on file for 90 days
- Remote hands to perform tape rotations and hardware swaps
- Constant management of all environmental systems (power, HVAC, fire, security and IDS)
- Remote monitoring of client equipment
- Locking cabinets and/or cages, Colo4 retains all keys
- Motion detection for lighting
- 30 inch raised floors
- 300 lbs/sq ft floor load
- Redundant HVAC with Liebert air handlers
- Each CRAC unit supported by independent roof mounted condenser
- Wind roof rating FM-90
- 11.1 MW of utility power
- 250 watts/sq ft
- Four (4) autonomous N+1 power plants delivering true A & B power supply
- Four (4) backup diesel generators on standby
- Generators tested bi-weekly and routinely run at full load
- Cabinet laid out for optimum airflow - hot and cold aisles separate exhaust and intake
- Solid cabling routed neatly overhead
- Ambient temperature of 70 degrees
- Pre-action dry pipe fire suppression
- Integrated smoke/heat detector system

Application Security

The application uses encrypted passwords in a POSTGRES database and does not give anyone access to passwords. There are no shared accounts, and Ethnio does not have access to login credentials for any users. We can reset passwords but that's it.

Automated Security Scans

We currently run several automated security scanning tools, and run reports at least once per quarter, but often more frequently than that, especially if we're deploying major features.

Automated Scans: **1x Quarter**

Reports Available Upon Request

External Penetration Tests

Once a year, we hire an outside firm to run an official penetration test. Most recently, that was Include Security, but we can use another vendor by customer request.

External Penetration Test: **1x Year**

Reports Available Upon Request

Code Review

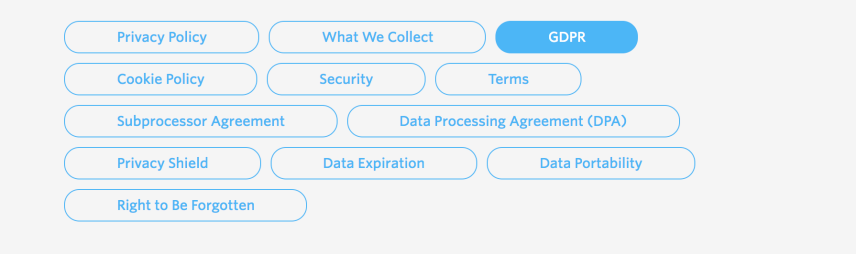
Since we're such a small team, all code is reviewed by pretty much everybody. With two developers there is no chance for any code to make it into the application that is not authorized.

Compliance with Security Standards

We don't have a formal process for ensuring compliance with security standards, but since applying the latest patches to NginX, Ruby, MySQL, and Rails is most of the battle, we are fairly obsessed with making sure our servers always have the latest patches applied. Developers are trained in security standards as much as possible, and we retain the services of Altoros to assist with that as well.

GDPR Compliance

Ethnio is in full compliance with GDPR. Read more here: https://ethn.io/gdpr



Privacy Shield

We like the EU and their privacy principles and make every effort to remain in compliance. The Privacy Shield framework has some expensive steps hidden inside the process, so although we meet all standards they outline, we haven't forked over the $5,000 to TrustE for the official external verifications. If you need that compliance, we can include that as part of any integration.

Privacy Shield Framework

Data Transmission

Each customer can choose to access Ethnio via SSL and issue their screener code via SSL. Ethnio maintains an updated certificate and can require secure access at customer's request.

Information Security Policy

Data Handling & Disposal

Industry best practices, along with automatic data expiration options per GDPR above.

Development Environment

We use a secure Github repository - industry standard.

Security Hardening

With only the SSL-encrypted Github repositories, Pivotal Tracker task management, and Rimuhosting secured data facility in Dallas, the Ethnio system has the most limited points of vulnerability. We can offer a Tripwire audit at additional cost.

Change Management - SVN

Ethnio uses Subversion to manage change in the codebase - also industry standard.

Remote Access

The only remote access to ethnio servers is through the SSH - each of the three developers has a unique key and access is closely monitored. We do not require two factor authentication mechanisms

Mobile Device Access

No Ethnio employees (there are only four) can gain access to ethnio servers using their mobile device.

Vulnerability Management

We monitor which ports are exposed to outside access, and track any sudden changes.

Employee Access

If an employee is terminated, accounts are immediately removed from all data sources - Rimuhosting, Pivotal, Github, etc. Device wipes are performed manually. We're not Google, for pete's sake.

User Account Administration

Issuing Accounts

There are three types of accounts in the Ethnio infrastructure - application accounts available to the public, paid accounts, and administration accounts. Administration accounts are only issued to Ethnio employees and require encrypted passwords. The other two account types allow user-selected passwords and are stored with a hash in the MySQL DB. The identity of users must be authenticated before providing them with account and password details.

Password Changes

We do not send passwords via email but offer unique password reset links - standard industry best practice.

Shared Accounts

Use of shared accounts is not allowed, but pursuant to the reality of the internet, we don't use IP-tracking to prevent this practice among our users, since it's unreliable.

API & System Standards

Access to Ethnio via secure token in the API may grant access to certain customer-defined data associated with a given screener, but that is entirely up to each customer and their user of the API. For example, if customer wishes to send responses from a screener to UserTesting.com, Ethnio may pass that data securely. More information on this can be found here: help.ethn.io

Account Cancellations & Permanent Deletion

For any permanently cancelled Customer account, Ethnio will automatically and permanently wipe all customer data from all servers within 24 hours of account deletion, including backup servers and sub-processors. Customer will receive email notification immediately upon deleting their account.

Access Requests

The only approval process for handling system or application access requests is that Nate has to approve each one. Accounts are reviewed constantly because there are only three administrators.

SOC2/SAS 70 Audits

Ethnio uses a TierPoint-managed facility where yearly audits are conducted. We don't track specific dates, but per the physical security section in this document, TierPoint provides these audits regularly. More information on the exact dates can be had by contacting: http://www.tierpoint.com/

Disaster Planning

PHYSICAL FACILITY

Remote backups are performed regularly and stored in a different physical location from the main servers. Colo4 and Rimuhosting provide UPS, generators, and real-time monitoring like crazy.

DATA SAFETY

All company information, design, and code management is stored redundantly across several locations.

MAXIMUM ALLOWABLE RECOVERY TIME

Hey it's a disaster. We're three people. We'll go as fast as we possibly can.

DISASTER SIMULATION AND TESTING

We never have, but if you want to pay for it, we'll simulate and test away. Earthquake, fire, or hurricane?

Custom Penetration Tests, Audits, and Vulnerability Scans

Ethnio has conducted several external audits by Include Security, Tripwire, and other 3rd party security assessment firms at the request of customers, with customers paying for that audit. Contact info@ethn.io to make a request.