SECURITY POLICY

Visible Network Labs ("VNL", "we", "our", "us") developed the visiblenetworklabs.com and partnertool.net websites ("Website", "Services") to help you solve complex problems through our comprehensive platform that provides all the tools, data and services in one place to help you measure, visualize and track key relationships and connections (personal and inter-organizational). We understand how important securing your is and we take reasonable steps to protect your information as if it was our own. If you would like a copy of our internal security polices please email us at security@visiblenetworklabs.com.

All communication between your browser and our servers is encrypted over HTTPS. Data is recorded into a MySQL database running on a password protected HIPAA-compliant Google Compute Engine server located in the United States. The data is only accessible through the visiblenetworklabs.com web interface and requires a valid login. The web interface has a valid SSL certificate so that no clear text data will be transmitted.

Our web interface has three access levels with varying levels of access to data:

- **Administrator**: users in this role are able to see all data for all users. Administrator accounts are limited to VNL employees.
- **Manager**: users in this role are able to see all data for all networks that they have created surveys for.
- **Respondents**: users in this role are only able to see the data that they individually contributed to the network’s dataset.

Unless a manager opts-out of inclusion, data are added to our larger dataset of cross-sector interorganizational data. We retain all the data, coded by their organizational names. As a result, we maintain the largest whole network dataset collected uses the same survey and methodology. We use that data to conduct descriptive and inferential analysis in exploration of cross-sector network impact and effectiveness. We value privacy at VNL and can make any exceptions or exclude your data altogether if you prefer not to contribute to this larger dataset.

- You can notify us at any time to destroy all records of your data from the dataset at any time. We will not do this unless we get a request in writing from you.
- You can opt-out of inclusion in the larger dataset if you so choose. Please notify us of your election to opt-out in writing.
- We do not routinely destroy the data.
- All data is backed up daily and the backups are retained for a minimum of 30 days.

All payments are securely handled with full PCI-compliance through Stripe, the industry standard. We do not store any sensitive billing information on our own servers. We do not receive or store credit card information into our servers. These transactions and Stripe’s use of your personal information is governed by their privacy policy (available at stripe.com/privacy).
VNL has in place a comprehensive incident management plan designed to respond and inform users of any event where their personal information of may have been compromised.

**Data Security Policy Changes**

Although most changes are likely to be minor, Visible Network Labs may change its Security Policy from time to time, at Visible Network Labs’ sole discretion. Visible Network Labs encourages visitors to frequently check this page for any changes to its Security Policy. Your continued use of this site after any change in this Security Policy will constitute your acceptance of such change.

Effective Date: March 9, 2018

**Questions?**

If you have any questions about our security policy, you can contact us by email at security@visiblenetworklabs.com or by mail using the following address:

By mail:
Visible Network Labs Inc.
Attn: Privacy
1536 Wynkoop St, Suite 913
Denver, Co 80202