Data Security Statement

Effective date: August 21, 2019

This statement explains J.Thelander's data security policies and practices with regard to the Thelander Platform (the "Platform"). We are responsible for ensuring the safe operation of the Platform. If you have any questions, comments or concerns about this statement or the Platform, please contact us at info@jthelander.com.

PLEASE NOTE ALL DATA CONTAINED IN THE PLATFORM MAY ONLY BE USED FOR BUSINESS PURPOSES BY AUTHORIZED USERS WITH A SUBSCRIPTION. ANY UNAUTHORIZED USE OF DATA WILL RESULT IN THE IMMEDIATE TERMINATION OF THE SUBSCRIPTION AND ACCESS TO THE PLATFORM WITHOUT A REFUND

Passwords and Credentials

- All credentials that enable access to the Platform are stored in secure systems that are only accessible to authorized staff.
- Passwords are only stored in the database in salted and hashed form and never in plain text form.
- You are responsible for preserving the confidentiality of your account password and will notify us of any known or suspected unauthorized use of your account. You agree that you are responsible for all acts or omissions that occur on your account while your password is being used.

General Security Practices

- All employees are trained on our policies regarding information and data security.
- Only personnel with a need-to-know basis have access to the data contained in the Platform and may restore data from backup data sets.
- Only authorized users (i.e., those with a paid subscription or who have participated in a survey) may access the Platform.
- We monitor and respond to active and emerging security threats.
- Security updates are applied within seven (7) days in non-emergency cases or more rapidly in the case of an urgent threat.
- Our system security is implemented according to industry standards.

Platform Security

- Access to the Platform happens through secure HTTPS connections.
- Access control lists define the behavior of any user of the Platform, and limit them to authorized behaviors.
- We run anti-fraud processes to detect malicious or harmful use of the Platform.

- All activity is logged to allow us to trace any security issues.

We provide this information as an explanation of our security practices, generally. These practices may change from time to time, and we will update this when necessary.