inclusivity

Empowering Inclusive Cultures

# Inclusivity Data Privacy and Security Charter

inclusivity

# The Purpose of this Charter

At Inclusivity, we take your privacy and the protection of your information seriously. Whether you are completing a survey, participating in an interview, or contributing to a focus group, we are committed to keeping your data secure and confidential.

This charter outlines how Inclusivity collects, stores, and protects the data we receive through our assessment and consulting processes, and how this information is analyzed and reported to our clients.

## About Inclusivity Insight Inc.

Inclusivity is a Canadian consulting firm that helps organizations build high-performing, inclusive workplaces. Through data-informed insights, leadership development, and practical advisory services, we partner with clients to strengthen organizational culture, leadership, and performance.

Our team brings a diverse mix of expertise—including data science, leadership development, change management and business —to provide impartial, third-party analysis and guidance. We work with organizations across North America, helping them use data to inform decisions and drive sustainable culture change.

## Where will the data be physically located?

All data collected by Inclusivity is stored on secure local servers located in Vancouver, Canada.

Servers are protected by firewalls and are regularly updated with the latest security patches. Inclusivity does not store client or participant data on third-party cloud services without prior notice and consent.

## How is the data kept secure and confidential?

The data provided by employees is protected and encrypted at all times. No one from the client organization “the client” will be able to see/identify responses. Data is processed by Inclusivity in aggregate so no individual response can be identified.

For the security of survey data, the data is always encrypted using a hardware-accelerated AES engine built into our hardware. This encryption is performed with 256-bit keys tied to a unique identifier. Inclusivity complies with internal data security policies that are reviewed and updated periodically and follows data security best practices to ensure data is secure.

Throughout this agreement, Inclusivity will keep all personal information confidential and secure.

inclusivity

## How are reports to my organization generated?

Inclusivity analyzes data in aggregate form only. This means that individual participants cannot be identified in any report, summary, or analysis shared with the client organization.

- **For surveys:** Inclusivity aggregates responses so that no individual's answers can be viewed. Clients never have access to raw survey data or identifiable responses.

- **For interviews and focus groups:** Notes or transcripts are analyzed for key themes and trends. Quotes or examples may be included in reports, but will be anonymized and will not be attributed to any individual unless explicit consent is provided.

## Can individuals from my organization see my responses?

No. At no time, will anyone from "the client" see how an individual responds to a question. The data is collected, analyzed and aggregated by Inclusivity as a third party vendor. Your organization will only be provided the data in aggregate format.

## How is data reported to ensure confidentiality?

Inclusivity will only provide data to "the client" in aggregate so the responses are anonymous (i.e. no individual will be identified in the report).

To ensure the protection of survey responses, Inclusivity establishes a baseline for analyzing aggregate data. For organizations with fewer than 500 respondents, a minimum of five users (sample size) from a specific group will be required for data to be reported. If the sample size is fewer than five users, the data will not be disclosed. This threshold increases to a sample size of ten for organizations with 500 or more respondents.

## What happens to the data at the end of the agreement with Inclusivity?

While the agreement is in place between Inclusivity and "the client", the client can only access aggregate reports developed by Inclusivity. The client will have no access to the individual responses.

When the contract with Inclusivity ends, "the client" will no longer be able to access aggregate data and the entire data file (all users' data) will be immediately purged from Inclusivity stations.

If you have any questions, please contact : support@inclusivityinsight.com