TROJAN
CONSTRUCTION GROUP

# PRIVACY & DATA SECURITY POLICY

TROJAN
CONSTRUCTION GROUP

# Privacy and Data Security Policy

## Introduction

The Privacy and Data Security Policy (the Policy) outlines guidelines of Trojan Construction Group – Sole Proprietorship LLC (TCG) and its subsidiaries (henceforth referred to as the Group) to safeguard the confidentiality, integrity, availability, and privacy of Personally Identifiable Information (PII) and data security. The Group is dedicated to ensuring that legislative, regulatory, operational, and contractual requirements pertaining to privacy and data security are met.

## Scope

The Policy applies to all areas of the Group's business operations, covering all directors, executives, and employees working for or on behalf of the Group. It also extends to outsourced employees or seconded employees working for and on behalf of the Group. The Group encourages external parties (vendors/suppliers, contractors, service providers etc.) working with the Group to adopt privacy and data security policies per the Group's Supplier Code of Conduct.

## Policy Statement

The Group acknowledges the importance of data ethics and respects every individual's right to protect PII. The Group is both the data collector and data processor for information collected unless otherwise stated. The Group ensures transparency in its data collection practices and emphasizes user consent.

*Data Privacy*

The Group is committed to communicating the following information, at minimum, to concerned individuals or PII principals:

- Purpose for collection of personal information;
- Method of information processing;
- Controls for protection of personal information;
- Usage of tools such as cookies to collect personal information online;
- Details of information such as IP address, Domain information captured about the user;
- Sharing of information with third parties;
- User rights to access of personal information;
- Details to contact the Group for queries on processing personal information;
- The Group's commitment to privacy and security;
- Period for which the terms and conditions are valid;
- The Group's information security standards and practices; and
- Policy on external links.

*Type of Information Collected*

The Group collects data that an individual provides directly to the Group via electronic or physical means including, but not limited to, PII and non-personal data, and data that is passively or automatically collected such as information collected from the individual's browser or device. The Group endeavors to obtain explicit consent when required and aims to inform individuals of the type and purpose for information collected. The Group aims to collect only the information it requires to conduct its business, establish, and maintain business relationships, and communicate with the individual. For security purposes, the Group has camera surveillance at its premises. The Group does not outright collect information on nor is any of its official channels directed towards children in accordance with laws and regulations in the jurisdictions in which it operates.

*Processing of Information Collected*

The Group will not use information about user activities on the Internet together with any information that would result in user being identified without his/her consent. The Group will not associate the information collected by software utilities (cookies, single-pixel GIF images) with username or email address, at the time of the user visiting the sites. The Group may use user identifiable information to investigate and help prevent potentially unlawful activity or activity that threatens the network or otherwise violates the user agreement for that service.

All kinds of data such as PII shared by users shall be:

- Processed fairly, lawfully and securely; and
- Processed in relation to the purpose for which it is collected.

*Data Security and Confidentiality*

The Group will implement guidelines to safeguard the privacy of the user's identifiable information from unauthorized access or improper use and will continue to enhance security procedures as new technology becomes available. The Group considers evaluating the implementation of an Information Security Management System that is aligned with the International Organization for Standardization (ISO) 27001:2022 standards.

The Group considers the following techniques in protecting PII and safeguarding the identity of the individuals whom it holds data on:

- Key-based encryption;
- Voiding or deleting characters within the dataset;
- Varying numbers and dates;
- Replacing values across the data; and
- Hash-based value masking.

In addition, the Group considers the following avenues when strategizing its approach to privacy and data security:

- Implement masking techniques that only reveal the minimum amount of data to anyone who uses it;
- 'Obfuscating' (hiding) certain pieces of data at the request of the subject, and only allowing certain members of staff to access the sections that are relevant to them;
- Building their Privacy operation around specific legal and regulatory guidelines; and
- Where pseudonymization is implemented, the algorithm that is used to 'de-mask' the data is kept safe and secure.

*Data Masking*

The Group considers the implementation of the following data masking techniques, such as pseudonymization and anonymization, to safeguard individuals' identities. Furthermore, the Group uses strategies like random substitution, format-preserving encryption, tokenization, masking, and redaction to ensure data security.

*Data Retention and Disposal*

All kinds of data such as PII shared by users shall be retained for no longer than is necessary for the purpose for which it is collected. The Group aims to dispose of data securely upon expiration of retention periods.

*Data Sharing and Third-Party Service Providers*

The Group does not sell or rent data. When the Group uses other agents, contractors, or companies to perform services on its behalf, the Group will ensure that the company protects confidential commercial/financial data consistent with this Policy.

*Individual Rights and Consent*

The Group believes that individuals should have the right to access, correct, or delete their data in accordance with laws and regulations of the jurisdictions in which it operates. The Group encourages individuals to contact the Group on its official channels pertaining to concerns on their data that is collected and stored. The Group will honor requests from user to review all PII maintained in reasonably retrievable form, which currently consists of the name, mailing / postal address, email address, telephone number and will correct any such information which may be inaccurate. Users may verify that appropriate corrections have been made. All kinds of data such as PII shared by users shall be maintained up to date and accurate as necessary.

Should requests be made to the Group to not continue using their information to provide individuals with services, the Group will delete concerned data from its data storage systems in accordance with its disposal methods. However, the Group shall retain necessary information to comply with laws and regulations in the jurisdictions in which it operates.

Users shall be provided with at least the following information before collecting PII:

- Purposes of processing the information;
- Any further information regarding the specific circumstances in which personal information is collected, such as:
    - The recipients of the information;
    - Whether submission of information is obligatory or voluntary, as well as the impact of failure to submit such information;
    - The existence of the right to access, update or remove personal information; and
    - Whether personal information will be used for marketing purposes.

*Privacy Breach Notification*

The Group aims to notify affected individuals and relevant authorities as required by applicable laws and regulations in the jurisdictions in which it operates in the event of a privacy breach. The Group is committed to setting up suitable communication pathways, which may include IT support teams and an online portal. Proactively, the Group strives to enforce procedures that monitor and manage privacy infringements and aim to prevent reoccurrences. The Group employs a variety of external technological solutions to amplify its services and ensure the optimal experience for its users. Even though it prioritizes collaborating with renowned and trusted external parties, the Group highlights that it cannot be held responsible for violations or security breaches on these external platforms. Nevertheless, the Group pledges to maintain a proactive approach to data protection and collaborate closely with its external parties to manage potential complications. The Group advises its users to be vigilant in defending their personal information, while it considers all efforts to safeguard it. The Group suggests that users adhere to online safety standards, such as creating robust passwords, activating two-factor authentication when possible, and immediately alerting the Group about any unusual occurrences.

*Third-Party Links and Sites*

The Group's official channels may contain links to external sites. The Group is not responsible for the privacy practices of these sites. The Group encourages individuals to be aware when they leave the Group's sites and to read the privacy policies of other sites.

Additionally, the Group operates pages and accounts on social media sites to engage with users. The Group is not accountable for content on these platforms that is not released or published by the Group. The Group urges individuals to read the privacy policies of these sites and discern between information originating from the Group and other sources. The Group does not vouch for the external platforms it utilizes, nor for the content disseminated by third parties on these platforms.

TROJAN
CONSTRUCTION GROUP

**Stakeholder Engagement**
The Group fosters close relationships with key stakeholders so that there is a clear understanding of their privacy concerns. Through stakeholder engagement, the Group identifies privacy factors that are important to stakeholders and integrates these considerations into this Policy.

**Training and Awareness**
The Group is committed to continuously investing in the training and development of its employees on matters pertaining to privacy and data security. The Group aims to regularly instill awareness and promote a clear understanding of the principles outlined in this Policy, empowering individuals to uphold these standards and mitigate risks effectively.

**Compliance**
The Group ensures regular monitoring of its activities for compliance with applicable laws and regulations in the jurisdictions where it operates. The Group undertakes internal audits of its privacy and data security practices annually, reporting the outcomes to relevant stakeholders and seeking external audits to align its commitments with industry standards.

**Roles and Responsibilities**
The Chief Executive Officer (CEO) is responsible for setting the Policy (including any revisions thereof) and monitoring its compliance. The Information Technology (IT) Manager is responsible for the implementation of this Policy and continuous improvement as well. All individuals working for or on behalf of the Group are responsible for upholding principles set forth in this Policy.

**Reporting and Transparency**
TCG encourages stakeholders to report concerns, suspicions, or potential violations of this Policy.

**Policy Review**
The Group believes in continually improving its performance from all the activities it undertakes or services it provides. The Group will review this Policy if and as required, and revise this to ensure it remains up-to-date and aligned with the company's Mission, Vision, core values, laws and regulations of the host countries of its operations, and with global best practices. The Group shall make available on the appropriate channels any changes to this Policy, and every version will have an updated effective date. Stakeholders are advised to refer to the Group's official channels for the most recent Policy.

This Policy was last reviewed in October 2023.