TOP NOTCH
Computers & Repairs • Commercial Technology Services
"Premium IT – Full Service"

Policy/Principles of Data Privacy and Governance

1. Introduction

Top Notch Group, LLC is committed to protecting the privacy and security of our clients' data. This policy outlines our approach to data privacy and the measures we take to safeguard sensitive information. By engaging our services, clients agree to the terms and practices described in this policy.

2. Data Collection and Usage

We collect and process data necessary to deliver our IT services effectively. This may include personal information such as names, contact details, and technical data related to our clients' IT infrastructure and systems. Data obtained through commission of service shall be used for diagnostic purposes only, and no information will be shared with third parties aside from our approved consultants and vendors list (see below).

3. Data Custody and Security

Industry-standard procedures have been taken to implement stringent security measures to protect client data from unauthorized access, disclosure, alteration, and destruction. These measures include, but are not limited to:

- Encryption: Client data is stored and transmitted using encryption protocols to ensure confidentiality.

- Access Controls: Access to client data is limited to authorized personnel only, and access rights are granted based on the principle of least privilege.

- Data Backups: Regular data backups are performed to ensure data integrity and availability in the event of data loss or system failure.

- Physical Security: Physical access to data storage locations is restricted and monitored.

4. Data Access Controls

Access to client data is granted on a need-to-know basis. Employees undergo background checks and sign confidentiality agreements to protect client data. Access to client data is logged and monitored for security purposes.

5. Data Privacy, Storage and Retention

Client data is retained for the duration necessary to fulfill the purpose for which it was collected, in compliance with applicable laws and regulations. Once data is no longer required, it will be securely

deleted or anonymized. We integrate privacy and security considerations into the development and implementation of our IT services, applications, and processes.

6. Third-Party Relationships

We may engage third-party vendors, partners, and consultants to deliver certain services on our behalf. Analysis is performed on their general information security posture. We ensure that they adhere to the same level of data protection as outlined in this policy through contractual agreements.

7. Response to Breach or Compromise

In the event of a data breach, a comprehensive incident response plan is utilized, commensurate with our insurance policies and industry regulations. We will promptly assess the breach, take necessary steps to contain and mitigate its impact, and notify affected clients and regulatory authorities as required by applicable laws.

8. Compliance and Legal Requirements

We are committed to complying with all applicable data protection laws and regulations, including but not limited to GDPR, CCPA, and any other relevant regional or industry-specific requirements.

9. Employee Awareness Training and Continuing Education

All employees undergo regular data privacy and security training to stay aware of the latest policies, procedures, and best practices for protecting client data.

10. Accountability & Periodic Review

Our privacy officer responsible oversees the implementation and enforcement of this policy and addressing data privacy-related concerns. This policy will be reviewed annually, updated as necessary to stay in line with changing regulations, technologies, and business practices.

11. As of (last revised): 12 June, 2023

For any questions or concerns regarding our Data Privacy and Custody Policy, please contact us.