Whitsol Ltd Data and Privacy Policy

Whitsol Ltd, a Ltd company registered in England and Wales, Trading as The Good IT Company, Vibe Websites and Engild Digital (The Provider), is required by law to provide information relating to how we handle personal details and information of our customers and associates (The receiver). This working document may be amended from time to time.

For the purpose of providing IT support:

The provider may hold information making access to a user's device possible, without the express permission of the client on each occasion, known as unattended access. It is the responsibility of the receiver to make reasonable steps to protect the data on their network from access by unauthorised parties.

The provider takes the following steps to ensure security of the information required to access the remote support portal:

- Forbid the use of a saved password to access the platform.
- Share the password with suitably authorised individuals only.
- Implement random generation passwords of high complexity, immune to standard attacks.
- Log remote access requests to end user's devices.
- Insist on encrypted hard drives to prevent theft of these login credentials from hard drives.
- Implement a suitable device destruction policy on devices that may have, at any point, had access to the login credentials.
- Storage of access details which could be used to gain administrative access to customers data in a password protected SQL Database, with data encryption

For the purpose of providing web services:

The provider may hold information relating to a client's activities in a number of ways in order to deliver effective web services, namely:

- Storage of the receiver's data on a remotely hosted web server.
- Storage of the receiver's clients data on a remotely hosted web server.
- Storage of email communication for the purpose of providing an email service provision to the receiver.
- Storage of access details which could be used to gain administrative access to customers data in a password protected SQL Database, with data encryption

These services may be outsourced to other providers, depending on specific requirements of the project.

The provider takes the following steps to ensure protection of the receiver's data for web services:

- Strong Passwords for file access, not shared with the receiver without request.
- Strong Passwords for control panel access, not shared with the receiver without request.
- A dedicated firewall to reduce the impact of any attacks on the server which may compromise data
- A tiered data centre to provide certified protection against physical access to the server

It is the responsibility of the receiver to ensure that adequate passwords are used to protect end users email accounts and other services for which security is self-managed.

For the purpose of providing digital marketing services:

The provider may hold details required to access online services (social media, search monitoring etc) in order to provide a digital marketing service to the receiver.

The provider takes the following steps to protect this data:

- Storage of access details which could be used to gain administrative access to customers data in a password protected SQL Database, with data encryption

For the purpose of day to day administration and communication

In order to conduct its activities effectively, the provider may hold personal information relating the receiver. This information may be sensitive and include passwords and other identifying material which may useable to gain access to the receiver's systems or commit identity theft.

The provider takes the following precautions to protect this information:

- A policy of not providing personal information to third parties without consent
- A 'named officer' policy to carrying out amendments internal to the receiver's systems which may give unauthorised internal access to user's information (e.g. email forwarding, the named officer will be made aware of this occurring)
- Storage of access details which could be used to gain administrative access to customers data in a password protected SQL Database, with data encryption
- Encrypted storage and transmission of internal emails, with strong password policies, with message tracking facilities

Right of Access

You have the right to request:

- A confirmation that we process and how we process your personal data
- A copy of any personal data we hold relating to you

Whitsol Ltd will respond to such requests within 40 calendar days.