Registered Office (UK) LTD

Security Policy

Updated 23.05.2018

Introduction

Registered Office (UK) Ltd is committed to protecting our customer's privacy and personal information. Our websites and servers employ extensive security measures in place to ensure your personal and company information and credit card details remain secure.

When you create an account, place a new order or log into our client admin portal (theoffice.support) your data is protected by an encrypted connection "https". This means that all information sent from your computer to our server is encrypted.

We are GDPR compliant and promise we will never sell your details to a third party.

Payment Information

We do not manage or have access to your payment data. We work with WorldPay as our payment gateway to assist us not only stay compliant regarding Data Protection, but also to make sure that your critical data is kept safe. When you enter your payment details into our website, you are entering them into a WorldPay secure server. WorldPay privacy policy can be found here https://www.worldpay.com/uk/privacy-policy.

Secure Connections, we use SSL (Secure Socket Layer protocol)

We use strong, cross-platform compatible encryption. SSL is in use across all our websites. The Secure Socket Layer protocol was created to ensure secure transactions between a browser and a server. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions.

Password Encryption

Your password is encrypted. Encryption uses a special key to turn your password into a random string of text and can only be decrypted with the same key.

Server Security

Our dedicated servers are located in a high security data centre in the UK. On-site security guards, CCTV monitoring and biometric systems restrict access only to authorised personnel.

Our servers are protected at the gateway by two managed SonicWall NSA Firewalls with Unified Threat Management (UTM), Deep Packet Inspection, Intrusion Prevention System, Gateway Anti-Virus, and DoS protection.

The Firewalls are in a high availability pair with automatic fail-over for maximum uptime.

All ports are blocked, and essential ports opened. Sensitive ports can be opened to specific IP's only in addition the server has a number of security features including a Web Application firewall which analyses all data being posted to the web site for signs of attack and blocks them.

An anti-brute force firewall will block brute force login attempts to our server and websites.

Managed Access

Only the minimum number of people necessary have access to our servers and network infrastructure.

Access privileges are granted based on roles and specific needs. Strong password controls are defined on each of our servers, websites and portals.

Cloud Based Data Storage

Our custom-built company management software is a cloud-based system – your data is stored in our database held in our high security data centre. This means that your personal and company information is not held on a PC, laptop or office server – all of which are all vulnerable to data loss or theft. For extra safety, regular backups are taken of your data.

Data Protection (backup and recovery)

For data backup and recovery purposes regular data backups are performed and held in storage systems within the data centre. All data backups are held in the UK

If you have any further questions or concerns regarding the security of our website(s), please contact us at: help@theoffice.support.

Updated: 23.05.2018