Qwarie
everything OSINT

Address: P.O. Box 683 Taunton
Somerset TA1 4ZX
Email: info@qwarie.com
Phone: +44 (0)3300 011161
Fax: +44 (0)1823 475310

Qwarie Security Policy

Introduction

The purpose of this policy is to ensure that Qwarie implements and maintains technical and organizational measures to protect Personal Information that it holds about customers, suppliers and employees.

Qwarie security measures include a complex set of technical and organizational, procedures and policies to ensure the best level of protection and security against unauthorized access, accidental or unlawful loss or destruction, modification, theft or disclosure of Personal Information.

Policy Statement

Qwarie is committed to preserving the confidentiality and integrity of all information it holds and processes to operate its business, in compliance with the UK Data Protection Act 1998, and EU Regulation 2016/679.

To read or download all our compliance documentation, please go to https://www.qwarie.com/documents

Security Measures

So that we are compliant with the legal requirements for the safe keeping of data and information, Qwarie has developed and implemented a series of organizational and technical measures.

On an organizational level, the following security measures are implemented:

- Access to the company premises is by dedicated swipe card and restricted to employees that have clearance to work there. This entails swipe card technology to the premises and a system that records when and by whom the room was accessed. These access records are reviewed by management regularly;
- Our after hours cleaners have access by dedicated swipe card and are vetted by our security company;
- We have human security on site during working hours and the building is locked down at night;
- Video surveillance system at the main access, work area and server room; suppliers are not permitted to progress beyond the reception area unattended;
- Access to the server room is restricted to designated approved personnel who are key holders;
- Mobile storage media is forbidden (CD / DVD, USB Stick, Portable HDD);
- All employees access company computers with identification and authentication;
- All employees ensure that PC is logged off or locked;

- Employees have been trained in all matters of data processing compliance. This includes the movement of such data, the security requirements for processing the personal data as well as the confidentiality on them; For additional information, please revert to our Data Protection Compliance Statement.
- On a technical level, the following security measures are implemented:
- Qwarie owns and operates a range of Virtual Private Networks for all external access to the WAN;
- SSH access is protected through key-based authentication only and non-standard ports;
- firewall, only the ports that need to be exposed are exposed;
- Use of a secure socket layer (https) on all Qwarie websites;
- Connections to servers that don’t have to be world-accessible are only allowed from specific countries; Also, Tor access is blocked on those servers;
- Strong passwords are applied to all systems and applications; we use a password manager to generate passwords no less than 28 characters long which include numbers, symbols, lower and upper case letters;
- Access by any user to any database that holds personal information is observed by live monitoring and recorded in a log file that identifies the person who has accessed the database, date of access, time of access and the type of operation performed;
- Functionality of applications used to process personal data and the type of user access is verified regularly by our IT Department;
- Backup of any database that holds personal information is performed constantly by our IT Department;
- Wi-fi connections are secured and controlled by our IT Department; for guest and employees that are not logged in to their work station (e.g. on a break), the company provides an independent wi-fi network;
- Bluetooth functionality is disabled on all company computers and devices;
- All data that is stored on a Qwarie server is encrypted; all data that is transferred is encrypted by default and only unencrypted at customer request;
- Access to employees’ personal e-mail suppliers such as Gmail and Yahoo mail is explicitly forbidden and prohibited;

Notification of changes to this policy

From time to time we may make changes to this Security Policy to reflect any changes to our security practices in accordance with changes in legislation, best practice and technology enhancements. If you wish to be notified of changes to this policy, please subscribe to our e-mail list.