Policy for IT Security and Integrity

Using the Worldfavor Services

Policy for IT Security and Integrity using the Worldfavor Services

“User” in this text refers to the company registered for using a company/organizational Worldfavor user account through worldfavor.com.

“Worldfavor Services” or just “Services” in this text refers to all technical services and its functionality provided to company/organizational users as accessed through worldfavor.com or any of its sub-pages, with or without charge.

Commitment to strong IT security

For Worldfavor, keeping our Users' information secure is one of our highest priorities. Worldfavor’s policy is to always use the best suppliers and routines possible to ensure quality and IT Security for data storage, data transfer and server management. Worldfavor is continuosly improving security practices, and this document is merely a description of current efforts.

For managing and maintaining the Worldfavor Services, accessible through worldfavor.com, specifically data storage, operation of servers and communiction of data through the Worldfavor infrastructure, Worldfavor is using the Microsoft Azure hosting services provided by Microsoft. This supplier and its services were selected because of its advanced and serious commitment to IT Security. Complete information about Microsoft Azure's IT security is available at: http://www.windowsazure.com/sv-se/support/trust-center/

Worldfavor is responsible for ensuring that the Services, accessed through worldfavor.com, are provided with a high level of IT security for our Users.

To prevent unauthorized access to your User account, we ask that you use a unique and strong password which you do not share with anyone.

Process routines

Worldfavor’s work with IT Security follows the standard SS-ISO/IEC 27001 for information security.

Encryption

Encryption, Password Hashing

Worldfavor makes sure to prevent that our users’ critical identity data fall into the wrong hands. We never store passwords as clear text - they are always hashed (and salted) securely using bcrypt.

Both data at rest and in motion is encrypted - all network communication uses TLS with at least 128-bit AES encryption. The connection uses TLS v1.2, and it is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism. Qualsys' SSL Labs scored our supplier Auth0's SSL implementation as "A+" on their SSL Server test.

Transparent Data Encryption (TDE)

Worldfavor uses Transparent Data Encryption to store sustainability data added by Users. TDE performs real-time I/O encryption and decryption of the data and log files. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an EKM module. TDE protects data "at rest", meaning the data and log files. It provides the ability to comply with many laws, regulations, and guidelines established in various industries.

Data in Motion between clients and servers

Worldfavor uses HTTPS (Hypertext Transfer Protocol Secure) with TLS 1.2, to ensure secure communication of data between clients and the servers. HTTPS ensures authentication and protection of the privacy and integrity of the exchanged data. The connection is encrypted with AES_256_CBC, with HMAC-SHA1 for message authentication and ECDHE_RSA as mechanism for key exchange.

Backup

Backup of User data is made every hour and saved for 30 days. If a User deletes data by accident, or if data is lost for any other reason, the user can receive backup of their data made within the last 30 days. If data is lost because of a mistake by the User, the delivery of backup will come with an extra charge.

Deletion of user data

The User has the right to delete data that they have added themselves through their user account. The data deleted by the User will be deleted from Worldfavor's servers after 30 days.

Data ownership and usage

The Users of Worldfavor are the owners of the company information they themselves have added to their Worldfavor account, and can at any time delete this data from the account. Data which has been deleted will be saved for 30 days in Worldfavor's servers for backup and restoration purposes and will after 30 days be completely removed from the servers.

Unless the User has chosen to publish data to the Worldfavor global public database, or through any other channel shared data from their Worldfavor account to a party outside of their own User account, the data is only accessible to those individuals who have access to administer the company's/organization's User account.

If the User has chosen to visualize or send any data to a party outside of their own User account, through any of the different methods and channels available using Worldfavor, that data will be accessible to those individuals who have access to the channel/method used. If the User has chosen to publish data to the Worldfavor global public database, the published data is accessible to anyone accessing the Worldfavor public database through Worldfavor.com, which could be other companies/organizations or private individuals.

Worldfavor will never disclose a User's unpublished/unshared data stored in a User account to a third party unless the User has actively chosen this. In case of a request from legal authority to omit the data, Worldfavor may disclose the User's contact information in order to refer the authority to contact the User directly.

To constantly improve the quality of the Worldfavor Services and develop new ones, and to deliver a useful, customized experience as well as guidance and insights, Worldfavor may process and analyze User data on an aggregated level based on all or a significant number of Users, only when data is aggregated and cannot be traced to a specific User or lead to conclusions about a specific User.

Employees of Worldfavor have acces to view data and User activity in User accounts, a possibility which only exists to ensure that the Services are developed, improved, maintained and overlooked in the best possible way to ensure high quality for our Users. This access only applies to employees who are directly involved in the above mentioned purposes. Employees who have access to data in User accounts are bound by the confidentiality of all information which is not published to the Worldfavor public database or in other way accessible to the public. Exceptions may apply if the User has approved an exception from this policy, or if Worldfavor employees communicate with a party who has been approved by the User to represent them.

Worldfavor holds the right to make changes in this Policy. We will not make changes that reduce your rights under this Policy without your explicit consent. We will notify you of any updates in this Policy through your User account and, if the changes are significant, we will provide a more prominent notice (such as email notification).

Security in development lifecycle

The development of Worldfavor's services follows strict processes to ensure a strong data security integrity. All development is done on a separate development environment, with a separate database, to make sure that no company or user data is exposed in any way to our development team.

Worldfavor's development is done in sprints and each sprint results in a new release/update. Each sprint follows a process with the mindset security first where all tasks and features are reviewed from a security perspective to find potential risks in advance and to mitigate to risk before development starts. Before each release/update we always conduct code reviews and run automated tests to ensure the security of the platform.