Effective Date 12/11/2019

FFS

Security

The following explain how we are trying to create a secure environment for your privacy and personal data. It applies when you visit our site or you use our Services as they are described in the Terms of Service and the Agreement that we may have.

FFS is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information and to ensure that appropriate security measures are in place to protect your Personal Data. We apply the security measures foreseen in the applicable regulations as well as our own technical and organizational security measures including policy, governance, procedures, responsibilities, risk assessment; network and sub-processor security.

FFS operates secure data networks protected by industry standard firewall and password protection systems. Our Security and Privacy and Personal Data policies are periodically reviewed and enhanced as necessary. Only authorized individuals have access to the information provided by our users. FFS takes steps to ensure that your information is treated securely and in accordance with this Privacy Policy.

Unfortunately, the transmission of information via the internet is not completely secure and so we cannot guarantee the security of your Personal Data transmitted through the Website; any transmission is at your own risk. Once we receive your information, we will use strict procedures and security features to try to prevent unauthorized access.

We treat the information you provide to us, including the Files, as confidential information; it is, accordingly, subject to our company's security procedures and corporate policies regarding protection and use of confidential information. After personally identifiable information reaches FFS, it is stored on a server with physical and electronic security features as customary in the industry, including utilization of login/password procedures and electronic firewalls designed to block unauthorized access from outside of FFS. Because laws applicable to personal information vary by country, our offices or other business operations may put in place additional measures that vary depending on the applicable legal requirements. Information collected on the sites covered by this Privacy and Personal Data Policy is processed and stored in Athens, Greece. However, because for some clients we act as processors, our clients may store their personal data in other countries and possibly other jurisdictions and in other countries.

All FFS employees are bind by our privacy and security policies. Your information is only accessible to those employees who perform technical support of the service.

If a password is used to help protect your accounts and personal information, it is your responsibility to keep your password confidential. Do not share this information with anyone. If you are sharing a computer with anyone you should always log out before leaving any site or service to protect access to your information from subsequent users.

FFS commitment to security is certified with ISO 9001 Quality Management Systems and ISO/IEC 27001 Information Security Management. For more information that is technical please see our security policy.

FFS operates in Greece (Athens) which is a member of the European Union, therefore it is GDPR compliant.

Below you may find technical information regarding how we protect your privacy and personal data:

- Data Hosting

Two Step Authorization

The FFS OTP and Google Authenticator apps provide one-time password codes for two-step authorization in FFS and other FFS products. Even if your password is stolen, your account will not be accessible to a would-be hacker.

- Your Data is Safe

Even in cafes, airports and other places with public Wi-Fi connections, passwords to FFS cannot be stolen. Users can confidently open FFS in public places through Wi-Fi or mobile network connections.

FFS is accessed exclusively through an SSL-encrypted connection, from initial authorization to the downloading and uploading of company data.

Proactive Protection

FFS has over 10 years of experience in providing the highest level of security for web projects. FFS benefits from all of this experience and technology.

- Office Security

FFS offices are secured via keycard access and video monitoring system. Access to FFS servers is permitted to a small number of FFS employees, requires OTP and is limited by source IP address. FFS maintains own cyber security department and uses external security consultants.

Available 24/7

FFS uses two independent data centers and High-Availability cluster architecture to make sure the service is maximally available.

- Backups

Reserve copies of data are created daily and replicated to an offsite location.

- OPERATING SYSTEM

At the level of the operating system, the FFS web server is behind a firewall where all ports are closed with the exception of those which are used for system purposes. Technical access to the server is carried out exclusively through FFS subnets.

- DATA STORAGE

All data centers used by FFS are protected in compliance with ISO 9001 Quality Management Systems and ISO/IEC 27001 Information Security Management standards (which include access to to the physical location based on proximity electronic security measures and 24/7 manned security All the physical media are encrypted. We try to build maximum protection against intrusion.

- DATA ISOLATION

User data (data of each company/client) is separated at the database and cloud storage levels. The data of different companies is isolated in such a way that there is no possibility of accessing data other than their own.

- WEB SERVER

A specialized server environment which does not allow write access to the local file system is used along with a customized PHP module which ensures isolation among users and security of user data.

- BROWSER LEVEL

Authentication data sent by a client machine can be encrypted using JavaScript and and RSA key. Additionally, OTP (one-time password) technology can be engaged in conjunction with an eToken.

- DATA TRANSFER

Data transfer for all users is carried out via an SSL-encrypted connection (with a 256-bit key).

- APPLICATION LEVEL

FFS' proactive protection blocks 100% of common attacks that arise from application code and is having protection against zero-day exploits: newborn malware which is not detected by any known behavior analysis. Malicious users do not have any opportunity to load malicious code via PHP. The web application conforms to WAFEC 1.0 standards. Access to FFS is provided to users (companies) in complete isolation from other users with passwords encrypted via md5. Limitation to specific subnets and logging of potentially threatening activity is also possible.