Fidesic

www.fidesic.com

FIDESIC DATA SECURITY POLICY

Table Of Contents

Introduction

Enliven Software (D.B.A. Fidesic) asserts that Information Technology is a critical component of both our daily business operations, and our core product. This policy seeks to ensure that Fidesic's IT resources and technology stack efficiently serve the functions of Fidesic as a company, and the security needs of our customers.

The Fidesic Data Security Policy is designed to protect both Fidesic and customer data such as:

- Customer company data such as names and addresses (email and physical) of the company, employees, vendors and customers
- Invoice data including invoice fields, due dates, payment terms, PDF copies of invoices and a log of all approvals
- Customer payment data including payment dates, recipients, terms, authorizations, and non sensitive payment reference numbers
- Sensitive payment data including bank account numbers and credit card numbers for both customers and suppliers.

All Fidesic customer data is stored in a secure Azure database, which is encrypted at rest. Access to this customer data is strictly controlled and limited only to Fidesic personnel who have a legitimate business need and the appropriate permissions. Sensitive data elements are further protected through additional security measures, such as tokenization or hashing, to minimize the risk of unauthorized access.

All computer equipment, peripherals, and software that are Fidesic property are provided for business purposes. Proper use and control of computer resources is the responsibility of all employees. Intentional, or reckless violation of established policies or improper use will result in corrective action up to and including termination.

This policy supersedes any previous Data Security policies of Fidesic, the following sections of Policy Statement, Disciplinary Action and Review and Acceptance apply to all individual policies contained within this document.

Policy Statement

It is the policy of Fidesic to use all IT related resources in a cost-effective manner that safeguards all internal and customer data. This includes data stored in our data environment, as well as all communications with current, potential, and past clients. The goal of this document is to comply with all federal and state regulations and protect the integrity of all data stored in our system. We also seek to protect sensitive information in a way to completely obfuscate this data from any and all users, therefore minimizing any risk associated with storing such sensitive information.

Disciplinary Action

Violation of any of these policies may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, any Board Member or owner who violates these policies shall be subject to removal. Additionally, individuals are subject to loss of Fidesic IT Data access privileges and may be subject to civil and criminal prosecution.

Review and Acceptance

The Fidesic Security Board shall review this comprehensive policy at least annually, making such revisions and amendments as deemed appropriate.

All Fidesic staff are responsible for review and acceptance of this policy annually. This policy will remain available to all staff, and appropriate communication of a reminder to review will be communicated to all employees.

Privacy Policy

Fidesic Privacy Policy is available on our website/product for all users to review. An updated version of this policy is available at https://app.fidesic.com/#/PrivacyPolicy

This policy has been built to meet GDPR standards for clarity and data privacy.

Asset Classification and Control

Responsibility and Ownership of Assets

All data stored in Fidesic's server environment is under the security control of Fidesic as a company. This includes internal Fidesic data as well as customer data. While Fidesic is the data security manager of all data within the Fidesic Environment, customer data remains the property of the customer themselves. Fidesic makes no guarantee that information provided by the customer, vendors, or client's customers is accurate.

Asset Classification and Control

- Public
    - This information is not sensitive in any way, and functionally is publically available. There are no restrictions, physical or virtual, to access this information. This includes but is not limited to customer logos and names.
- Client Data
    - This is all information available from the Fidesic product directly. This data is managed by our login control, and user roles for permissions within the system. All client data is segregated by company logins and inaccessible across client configurations.
    - This data is encrypted at rest.
- Fidesic Restricted
    - This information is to remain confidential and only available to Fidesic on a 'need to know' basis. This includes but is not limited to client lists, source code, internal documentation, server access, audit logs etc.
    - This data is secured behind logins with 2FA where applicable.
- Sensitive
    - This information is not available through any Fidesic interface. This data uses tokenization when possible and is encrypted at the column level as well as encryption at rest. Where applicable this data is hashed. This data includes client and vendor banking information including bank account numbers, credit card numbers, or user passwords.
    - This data is secured using Cybersecurity Best Practices Based on NIST Cybersecurity Standards.

Acceptable use of Information Systems

Acceptable Use

Access to any data within Fidesic is controlled by a user authentication system. Only users authorized through this system have access to data, and authorized users are accountable for all activity that takes place under their username.

Authorized users should be aware that data they create on the Fidesic platform will become subject to data asset classification above, and with the exception of sensitive information, it may be available to other authorized users of the site.

Fidesic reserves the right to audit networks and data on a periodic basis to ensure compliance with this policy.

For security and network maintenance purposes, authorized users within Fidesic may monitor equipment, systems, network traffic and non-sensitive data at any time.

Fidesic Internal Security Standards for Data Access

All Fidesic team members with internal access to restricted data must comply with this policy and the following security policies for personal computer security

- All users must access data through only an authorized user account
    - This account must have a secure password meeting internal standards
- All users must maintain a current operating system/browser at all times to ensure security
- All PCs that access Fidesic data must be secured with a local password.
- All users must access data over a secure wifi network, or VPN.

Unacceptable Use

Users may not intentionally access, create, store, or transmit material which may be deemed to be offensive, indecent, or obscene. Under no circumstances is a user, employee, volunteer, contractor, consultant or temporary employee of Fidesic authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Fidesic resources or data.

Human Resources Security

Employee Screening

In the United States, Fidesic currently uses an external screening agency to perform pre-employment background investigations for newly hired personnel. Personnel screening in other countries varies according to local laws, employment regulations and Fidesic policy.

Confidentiality Agreements

All Fidesic Employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their terms of employment. Fidesic obtains a written confidentiality agreement from each subcontractor before the subcontractor has access to any data.

Security Awareness Education and Training

Fidesic promotes security awareness and educates employees through regular training and security focused meetings. Each employee must review and agree to the Fidesic Data Security Policy on a yearly basis.

Database Security

All Fidesic data is stored in an Azure Cloud environment. The Azure cloud has no physical access for any employee of Fidesic, or any customer. Azure facility, premises and physical security information is available from Microsoft here: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

All virtual access to data is controlled through either Fidesic User Authentication, or in the case of the Fidesic Development and IT team, through operations management below.

Operations Management

Protection Against Malicious Code

Fidesic policy requires the use of antivirus protection, firewall software and VPN control on endpoint devices such as laptops, desktops. Any computer or virtual machine storing Fidesic data must have automatic security updates from Microsoft enabled. Security updates on all other devices must be installed upon notification of their availability.

Fidesic keeps antivirus products and Windows Server Update Services up to date with virus definitions and security updates. Fidesic will notify system users of any credible virus threats.

System Monitoring and Protection of Audit Log Data

Fidesic logs certain security related activities on operating systems, applications, databases and network devices. Systems are configured to log access to all virtual machines, as well as any system errors and console messages. Fidesic has implemented controls to prevent operational problems including log file media becoming exhausted, failing to record events and logs being overwritten.

Access to security logs is provided on a need to know basis, and where applicable logs are encrypted for added security.

Network Controls

Fidesic has implemented strong network security controls at all potential access points of data during transmission. For administration of network security and network-management devices, Fidesic requires personnel to use secure protocols with authentication, authorization and strong encryption.

Remote connections to the Fidesic network must exclusively use approved virtual private networks. Access to Azure settings and logs are also protected by two-factor authentication. Fidesic wifi-security policy forces all connections on wifi-connections to be done through secured networks.

Access Control to Source Code

Fidesic maintains strong security controls over its source code. Fidesic's policy places limits on access to source code (including enforcement of need-to-know), requirements for independent code review, automated testing, and periodic auditing of source-code repositories. Source code protection has two main priorities

- Protect Fidesic's customers against any malicious attempts to alter the source code to create security vulnerabilities
- Protect Fidesic's Intellectual Property

Access Controls

User Access Management

Access privileges are granted based on job roles and require management approval. Operations are organized into functional groups, where functions are separated by a group of employees. Functional Groups include developers, system administrators etc.

Password Management

As a part of the Fidesic Password policy, all users must create strong passwords for any account with access to Fidesic assets. This includes network access, email, database, and Fidesic itself. As a part of the Fidesic strong password policy, all passwords must be unique, and stored using an encrypted, password management system. This minimizes both the likelihood of unauthorized access and the impact of an event where a password is compromised. Employees are not permitted to re-use passwords they use outside of Fidesic.

Periodic Review of Access Rights

Fidesic regularly reviews network and operation system accounts to ensure appropriate access levels. In the event of employee termination, Fidesic terminates network access. Access permissions are managed, incorporating the principles of least privilege and separation of duties.

Information Data Security Incident Response

Fidesic information security response is based on the recommended best practices from the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources.

If a security incident is discovered, Fidesic will begin a rapid and effective incident investigation, response and recovery process. A root cause analysis is performed to identify opportunities for measures to improve the overall security posture. Fidesic will follow a formal chain of procedures to collect information, maintain a custody of evidence, and complete a full investigation (this evidence may include legally admissible forensic data when necessary).

If there is a confirmed security incident involving information and data stored that involves a Fidesic customer, Fidesic will promptly notify any affected customers of both the scope and potential impact of any such incident. Information about malicious attempts, suspected incidents, or incident history is confidential and not externally shared.

Information Security Resilience Policy

The Information Security Resilience Policy (ISRP) objective is to establish a business resiliency framework to help provide continuity in response to business interruption events affecting Fidesic's regular operations.

The ISRP approach is built upon several programs: emergency response, crisis management of incidents, technology emergency recovery and business continuity. The objective of this program is to minimize negative impacts to Fidesic customers and maintain critical business processes until regular operating conditions are restored. The Fidesic Information Security Resilience Policy is aligned with the business continuity and disaster recovery recommendations in the NIST Cybersecurity Framework.

The Fidesic ISRP is designed to engage several aspects of emergency management and business continuity from the onset of an event and adapt based on the needs of the situation.

Fidesic Security Assurance

The Fidesic Security Assurance program is designed to incorporate security controls and best practices from industry-leading frameworks, such as ISO 27001 for information security management and the NIST Cybersecurity Framework. By aligning our security efforts with these recognized standards, we aim to provide our customers with a level of assurance that their data is protected in accordance with leading practices.

Coding Standards and Security Training

All members of the Fidesic Development team are required to review, and follow our continually updated Fidesic Best Practice Coding Standards. These standards are designed not only to provide a consistent experience for our end customers, but to make sure all code introduced follows our strict security standards.

As a part of our development process all code must go through peer code review to assure it meets our coding standards for security.

Security Analysis and Testing

Security testing of all Fidesic code includes both function and non-functional activities for verification of product features and quality. These tests include all overlapping features, and provide comprehensive coverage for security coverage over all Fidesic products.

Quality Assurance is executed by the scrum master, product owner, as well as an automated QA system. All critical aspects of Fidesic are tested any time there is new code introduced. All QA is complete in a staging environment to avoid any potential impacts with customers.

External Standards for Compliance

Fidesic submits certain aspects of our system to external review for compliance. Our hosting provider for all Fidesic services, Azure, maintains a current SOC 1 report. Additionally, Fidesic undergoes regular PCI DSS compliance audits and vulnerability scans to ensure our systems meet the security requirements for handling payment card data. We also leverage the NIST Cybersecurity Framework as a guide for our overall security posture and controls.

External Site Scans for Compliance

- PCI Compliance and Scanning
    - PCI DSS SAQ - Enliven Software, LLC has demonstrated full compliance with the PCI DSS.
    - ASV scans are being completed by the PCI SSC Approved Scanning Vendor, ControlScan
- SSL Labs Scanning Regular Scanning for SSL Vulnerabilities
    - Overall Rating A+