FOND

FOND'S SECURITY AND PRIVACY POLICIES

Fond is a rewards and recognition solution that seamlessly consolidates your processes into one easy-to-use platform, so you can get back to doing what you do best: building an organization where employees love to work. With Fond, you can recognize and reward employees, access exclusive corporate discounts, and measure success, so your team spends less time wrangling programs and more time getting results you never thought possible.

Introduction

In a world where data security and privacy is more important than ever, software-as-a-service (SaaS) companies must constantly adapt to new regulations and policies to better protect customer data. At Fond, protecting our customers' data is our highest priority, and we believe our customers have the right to know when and how we use their data. As cloud computing becomes more widely accepted and leveraged, companies must become more transparent with how they treat customer data. This paper provides an overview of Fond's data security and privacy.

Regulatory Compliance and Certifications

Fond maintains a formal and comprehensive security program designed to comply with all applicable data privacy and transmission laws. Our security program ensures the security and integrity of customer data, protects against security threats or data breaches, and prevents unauthorized access to customer data.

SOC 2 External Audits

Fond's operations, policies, and procedures are audited regularly to ensure Fond meets and exceeds all standards expected of service providers. System and Organization Controls (SOC) reports are independent and annual third-party examination reports that demonstrate how companies achieve key compliance controls and objectives. SOC 2 compliance is the industry standard for SaaS companies, especially those working with large customers concerned with data privacy and security. Fond operates in compliance with SOC 2 to ensure your data is protected, available, and secure.

Fond publishes a (SOC 2) report that addresses the Security, Confidentiality, Availability, and Privacy principles of the Trust Services Principles and Criteria, which is available to all customers upon completion. The scope of SOC 2 covers any Fond system containing data the customer and its employees submitted to the Fond Service. The SOC 2 audit validates Fond's physical and environmental safeguards for production data centers, backup and recovery procedures, software development processes, and logical security controls.

The General Data Protection Regulation Act (GDPR)

GDPR is an EU-based privacy law that took effect on May 25, 2018, governing the ownership of data and data subjects (users). GDPR establishes guidelines for a user's rights to correct their data, remove their data, receive a copy of data acquired by companies, and have visibility into how their data is used. Under GDPR, organizations must disclose what data they capture, for what purposes, and what legal bases they have for capturing and processing data.

Fond believes GDPR is a necessary and important step to improve data protection for our customers' global employees, and we are excited to further strengthen our commitment to keeping your data safe. Fond's has updated our privacy policy for GDPR and established processes and technology for handling and managing data subject requests.

Cross-Border Data Transfers

To comply with strict data protection laws governing the transfer of personal data from the European Economic Area (EEA) to the US, Fond has incorporated the European Commission's approved standard contractual clauses (also referred to as the "Model Contract") into our data protection policies. The Model Contract requires that companies meet the adequacy requirement to allow for the transfer of personal data from the EEA to a third country.

Fond has also self-certified to the Privacy Shield, which is a self-assessment of how data is handled when transferred between countries. Our comprehensive privacy policy ensures your data is encrypted and secure.

Every attribute of customer data on the Fond platform is encrypted in transit and at rest using AWS RDS. Fond uses the Advanced Encryption Standard (AES) algorithm to encrypt data. Data inserts, updates, and deletions are committed to a persistent store on a MySQL database. With Fond, companies of all sizes can rest assured that we have taken every step possible to ensure your data is secure.

Physical Security

Fond hosts its production services at Amazon Web Services (AWS) across multiple regions. AWS limits physical data center access to approved employees or third-parties whose access is requested by approved AWS employees. In both cases, requestors are required to provide a valid business justification for entry. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Authorized personnel approve requests, and access is revoked after request time expires. Once admitted, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are then signed in and escorted by authorized staff.

Encryption of Data in Transit (Network Security)

Fond's internet is protected by Transport Layer Security (TLS), which secures network traffic from passive eavesdropping, active tampering, or forgery of messages. Fond also uses proactive security procedures such as perimeter defense and network intrusion prevention systems. Fond's network infrastructure is also tested for vulnerability by internal Fond resources and external third-party vendors.

Encryption of Data at Rest (Database Security)

Fond encrypts every attribute of customer data within our application when it is stored in our database. This is a fundamental design characteristic of the Fond technology. Fond relies on the Advanced Encryption Standard (AES) algorithm with a key size of 256-bits. All data inserts, updates, and deletions are committed to a persistent store on a MySQL database.

Backups

Fond uses the AWS Relational Data Service (RDS) using MySQL. Data can be restored from RDS to a given point in time, up to within five minutes of current time. RDS is configured to run full snapshots of production databases on a daily basis. Fond also takes additional nightly backups that are retained for one year.

AWS RDS backups and nightly backups are stored encrypted in the Amazon Simple Storage Service (S3), and are retained for seven days. AWS S3 data is automatically distributed in real-time to at least three geographically separated physical facilities within an AWS Region.

Disaster Recovery and Business Continuity

Fond is committed to providing the highest level of service availability. Fond's Disaster Recovery and Business Continuity (DR/BCP) plan includes a Recovery Time Objective (RTO) of four hours and a Recovery Point Objective (RPO) of 24 hours. Fond operates its service and its business exclusively in the cloud and all its services are fully redundant. In the event of an unscheduled outage or natural disaster, Fond executes its DR/BCP. The DR/BCP is tested at least annually.

Logical Security

Fond's security access is role-based, supporting SAML for Single Sign-On (SSO) and/or native username/password authentication for both user and web services integrations.

Single Sign-On (SSO) Support

Fond's native SAML 2.0 SSO enables an enterprise SSO environment. SAML allows for a seamless SSO experience between the user's internal web portal and Fond. Users log in to their company's internal web portal using their enterprise username/password and are presented with a link to Fond. This link automatically provides access to Fond without having to log in a second time.

Fond's Native Login

For customers who wish to use Fond's native login, Fond only stores the user's Fond password in the form of a secure hash, as opposed to the password itself. Unsuccessful login attempts are logged and locked after five failed attempts. Inactive user sessions are automatically timed out, and this feature is customer-configurable.

Password rules include: minimum length; alphanumeric values; cannot match last five passwords; and cannot contain repeating, ascending, or descending characters or patterns.