



# TeamsID Security Whitepaper

December 14, 2015 ©2015 SplashData, Inc. All rights reserved. v2015.12

# INTRODUCTION

TeamsID is from SplashData, a company that has a well-established track record of delivering password management and security solutions to millions of individual and business customers since 2000. Our infrastructure and security team includes people who've played lead roles in designing, building, and operating highly secure cloud based systems. Our long experience has taught us that maintaining security is an ongoing process and that no one organization can hope to be the best at all aspects of security. So we work closely with the best partners we can find -- like Rackspace for hosting and Stripe for payments -- that focus exclusively on maintaining leadership in their particular areas of security expertise. Most importantly, we respect your privacy and the security of your records. Everything we do at TeamsID is built around that respect and designed to maintain your privacy and security. We would never do anything with your data that we wouldn't be proud to tell the world about.

Millions of users trust SplashData and its security product SplashID to easily and reliably store, sync, and share sensitive information across devices. TeamsID brings that same simplicity to the workplace, with advanced features that help teams share instantly across their organizations and give admins the visibility and control they need. But although designed as an easy-to-use tool for management and and collaboration, TeamsID is also designed to keep important information secure. To do this, we've created a sophisticated base infrastructure upon which account administrators can layer and customize policies of their own. In this paper, we'll detail this infrastructure and our back end policies -- as well as the options available to admins -- that make TeamsID such a great solution for getting work done productively and securely.

As you continue to learn more about TeamsID, we recommend you also review our Terms and Privacy Policy.

### PERMISSIONS, ADMIN CONTROLS AND AUDIT

TeamsID provides administrative control and visibility features that empower both IT and end users to effectively manage their businesses and data. Below is a sampling of features available to team admins and users managing core IT processes.

No two organizations are exactly alike, so we've developed a number of tools that empower admins to customize TeamsID to their teams' particular needs. Below are examples of control and visibility features available via the TeamsID admin console. TeamsID enables organization admins to set permission levels for any employee with access to TeamsID. Permissions can be set for access to organizations, teams, records, or record editing. The following three access levels can be assigned to each user to enable more effective team management:

### **Organization Admin level:**

- Access to Organizational Settings
- Access to all Teams and Team Settings
- Access and edit permissions to all the records in the Organization (except each member's My Safe personal records)
- Download activity logs by user or Team or for the entire Organization

### **Team Admin level:**

- Access to the Team's Settings
- Access and edit permissions to all the records that are available to this Team

### **Team Member level:**

• Access to all records in the Team. A Team member can edit a record if "Record Editor" permission is given explicitly for a record.

# PRODUCT FEATURES

TeamsID is used for securely storing and sharing passwords in an organization. Here are some key features (and this list is always growing):

- My Safe store your personal records
- Teams manage users by adding/removing them to different teams
- Records store your password into records
- Assignments every record can belong to a user and/or to a team
- · Permissions (Note: permissions are set for least amount of access by default)
  - Permissions are set based on users or teams
  - Administrators have full permissions
  - The following permissions can be set for a user or team:
    - Can view
    - Can edit
    - Can delete
    - Can print
- Import & Export
- Mobile and desktop client apps
- Browser extensions
- Backups
- Self-hosted option
- Ability to install the application on your own servers and use from there.

# USER PROVISIONING METHODS

### Sign up

First step with TeamsID is creating an account. Creating an account is free. You can create your account in two ways:

- Sign up yourself. Then you can create a new Organization or get an invitation to join an existing Organization that uses TeamsID.
- Or you can first receive an invitation to join an existing Organization that uses TeamsID, and then when you create your account you will automatically become a member of that Organization.

### Authentication

First step with TeamsID is creating an account. Creating an account is free. You can create your account in two ways:

- Sign up yourself. Then you can create a new Organization or get an invitation to join an existing Organization that uses TeamsID.
- Or you can first receive an invitation to join an existing Organization that uses TeamsID, and then when you create your account you will automatically become a member of that Organization.

### **Password reset**

Individual user passwords are not stored anywhere on our servers at TeamsID. However, if a user forgets their individual TeamsID password, the user's Organization Admin can reset the password to re-enable access to shared Organization records. In this scenario, however, the user will lose all personal records inside their My Safe folder. Note that only the Organization Admin can reset a user password.

There are 2 ways to initiate a password reset:

- Option 1) User initiates it from the sign in page
- Option 2) Admin initiates it from Organization Settings (Members tab)

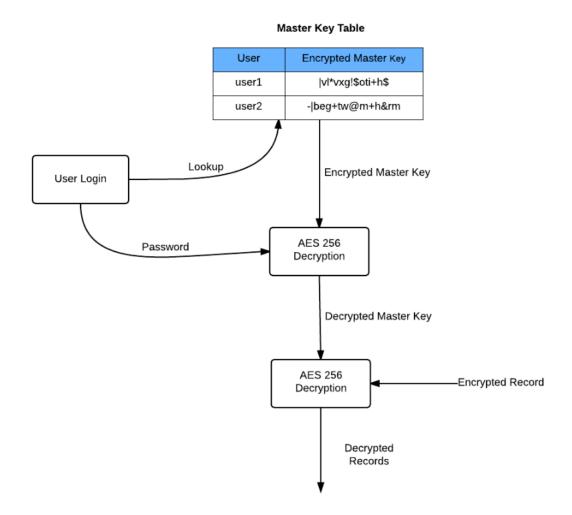
# SECURITY ARCHITECTURE

Despite our easy-to-use interface and apps, TeamsID is backed by a robust architecture to ensure fast, reliable, and secure operation. We're continually evolving our product and architecture to speed data transfer, improve reliability, and adjust to changes in our users' environments.

In this section, we'll explain how data is transferred, stored, and processed securely. TeamsID is designed with multiple layers of encryption, network configuration, and application-level controls that are all distributed across a scalable, secure infrastructure. TeamsID users can access records and folders at any time from the desktop, web, and mobile clients. All of these clients connect to secure servers to provide access to records, allow sharing with others, and update linked devices when records are added, changed, or deleted.

### **Security design**

TeamsID uses security mechanisms that go beyond traditional encryption to protect user data. TeamsID's security architecture is based on secrets known only to our users. We use AES 256-bit encryption and employ the user's password as the key to the encryption mechanism. The user password is never stored on TeamsID servers and must be provided by the user to decrypt the records. In order to be able to share records, multiple users must be able to decrypt the same record. To implement that we use an automatically generated master key to encrypt all the records of an organization, and then we encrypt that master key using each user's password. This model has many advantages, one of them enabling Organization Admins to be able to reset individual user passwords.



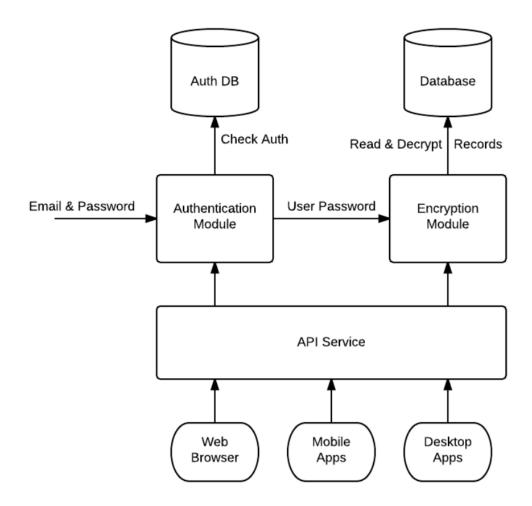


### **Encryption library**

TeamsID makes use of the php mcrypt library. We believe in the power of open source and trust its proven model over time and by different vendors. TeamsID uses the Rijndael cipher with CBC mode encryption. It has proven to be a reliable model, and we have used it successfully on other products with widespread user bases.

### System architecture

The TeamsID system architecture was designed with a modular approach. Here is a quick glance at what the architecture looks like.



The Authentication Module has its own database for authentication only. It is completely independent from Encryption and the only requirement for Encryption is providing a "secret" specific for each user, which in TeamsID's implementation is the user password. This modular approach allows the Authentication Module to be developed independently and even be replaced by a different module as long as the relation towards Encryption is maintained.

The Encryption Module ensures that records are stored in a safe manner and can be retrieved any time. It takes a single input from the Authentication Module and uses that input as the "crib" to the decryption process. The Encryption Module uses its own database for storing records and other application related information. This structure enables stricter and more secure methods of access and backup.

Our flexible design also allows the Encryption Module to be updated or even replaced depending on requirements. The API Service combines the Authentication and Encryption Module (but also other elements such as Account Management and Logging) and offers their functionality as a set of API calls that can be used by different clients such as the TeamsID web client and native apps.

# APPLICATION AND DATA SECURITY

The TeamsID service can be utilized and accessed through a number of application interfaces. Each has security settings and features that process and protect user data while ensuring ease of access. Security of the client applications that access TeamsID data is of equal importance to us as the security of the core application. Meanwhile, TeamsID sync mechanisms ensure fast, responsive anywhere access to data across devices.

- TeamsID web application allows users access to their records through any modern web browser.
- TeamsID Windows and Mac applications The TeamsID desktop application is a powerful sync client that gives users full access to their TeamsID records. Offline access on desktop apps is in development.
- TeamsID mobile applications The TeamsID app is available for iOS and Android, allowing users to access all their records on the go. The mobile app also supports favoriting of records. Offline access on mobile apps is coming soon.
- TeamsID Chrome browser extension allows users to view TeamsID records directly on the extension's interface. Users can also auto-fill and auto-login to websites.

### Data in transit

To protect data in transit between TeamsID apps and our servers, TeamsID uses Secure Sockets Layer (SSL) / Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. File data in transit between a TeamsID client (desktop, mobile, API, or web) and servers is always encrypted via SSL/TLS. For end points we control (desktop and mobile) and browsers, we use strong ciphers and support perfect forward secrecy and certificate pinning.

Additionally, on the web all authentication cookies are secure and enable HTTP Strict Transport Security (HSTS) with include subdomains enabled. To prevent man-in-the-middle attacks, authentication of TeamsID front-end servers is performed through public certificates held by the client. An encrypted connection is negotiated before the sync of any records and ensures secure delivery of data to TeamsID apps.

### Data at rest

TeamsID records at rest are encrypted using 256-bit Advanced Encryption Standard (AES). Records are stored in multiple data centers in discrete blocks. Each block is fragmented and encrypted using a strong cipher. User data is encrypted using the user's password. Organization data is encrypted using the auto-generated master key. Neither the user's password or the Organization master key is stored on our servers.

### **Certificate pinning**

TeamsID does certificate pinning in modern browsers that support the HTTP Public Key Pinning specification, and on our desktop and mobile clients in most scenarios and implementations. Certificate pinning is an extra check to make sure that the service you're connecting to is really who they say they are and not an imposter.

#### **Framework security**

The framework chosen to develop our system is Laravel. It is a modern PHP framework built with security in mind. Laravel uses Eloquent as its ORM to access databases. This minimizes the risk of SQL injection. It also provides a templating engine to protect against XSS attacks, and CSRF protection is automatically enabled for all forms.

# **RELIABILITY & INCIDENT RESPONSE**

### Reliability

A security system is only as good as it is reliable, and so we've developed TeamsID with multiple layers of redundancy to guard against data loss and ensure availability. Daily backups are performed on all data. TeamsID uses Rackspace systems that are designed to provide 99.99% durability. This feature, beyond protecting user data, ensures high availability of the TeamsID service. In the event of a failed connection to the TeamsID service, a client will gracefully resume operation when a connection is re-established. Records will only be updated on the local client if they have synchronized completely and successfully validated with the TeamsID service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

#### **Incident response**

We have incident response policies and procedures to address service availability, integrity, security, privacy, and confidentiality, including:

- Prompt response to alerts of any unusual activity
- Determination of the severity of the incident
- If necessary, execution of mitigation and containment measures
- Communication with internal and external stakeholders, including notification to customers
- Gathering and preservation of evidence for investigative efforts
- Documentation and analysis to develop triage plan and long term remediation plan

### **Business continuity**

We maintain a business continuity plan (BCP) to address how to resume or continue providing services to users as well as how to function as a company — if business-critical processes and activities are disrupted. Our BCP identifies internal and external threats and specifies how people, processes, and infrastructure will be mobilized to prevent and recover from disruptions.

### **Disaster recovery**

To address information security requirements during a major crisis or disaster impacting TeamsID business operations, we maintain a disaster recovery plan. The TeamsID Infrastructure team reviews this plan annually and tests selected elements at least annually. Relevant findings are documented and tracked until resolution. Our Disaster Recovery Plan (DRP) addresses both durability and availability disasters. A durability disaster is complete or permanent loss of primary metadata data centers, or lost ability to communicate or serve data from metadata data centers. An availability disaster is defined as an outage greater than 10 days, or lost ability to communicate or serve data from storage service/data centers. We define a Recovery Time Objective (RTO), which is the duration of time and a service level in which business process or service must be restored after a disaster, and a Recovery Point Objective (RPO), which is the maximum tolerable period in which data might be lost from a service disruption. We also measure the Recovery Time Actual (RTA) during Disaster Recovery testing, performed at least annually. TeamsID incident response, business continuity, and disaster recovery plans are subject to being tested at planned intervals and upon significant organizational or environmental changes.

#### **Data centers**

TeamsID corporate and production systems are housed at Rackspace data centers located in the United States. Rackspace is responsible for the physical, environmental, and operational security controls at the boundaries of TeamsID infrastructure. TeamsID is responsible for the logical, network, and application security of our infrastructure. Connections are protected through an IDS and Cisco firewall, which are configured to offer offer highest level of security and monitoring. TeamsID severely restricts access to the environment to carefully screened individual IP addresses and employees.

### SELF HOSTED ON PREMISES OPTION

TeamsID also offers a self-hosted on premise solution. For information on using this option for your organization, please contact our sales team at <u>sales@teamsid.com</u>.

# SUMMARY AND FURTHER INFORMATION

TeamsID offers an easy-to-use password management tool to help teams collaborate effectively while providing the security measures organizations require. With a multi-layered approach that combines a robust back-end infrastructure with a customizable set of policies, we provide businesses a powerful solution that can be tailored to their unique needs. To learn more about TeamsID, visit www.teamsid.com or contact our sales team at sales@teamsid.com.

Website - www.teamsid.com

Admin guide - guide.teamsid.com