# Trello Business Class

## Operations and Security Guide

# Introduction

Millions of people and thousands of businesses use Trello to work together and keep their important projects organized and on track. These businesses trust Trello to reliably store and securely provide access to their company data and files. This document details the services, policies, processes, and procedures that have been put in place to make Trello a secure and reliable service for all of our users. Additionally, this document provides an overview of the additional permissions and controls available to administrators of teams that have been upgraded to Trello Business Class[1] or Trello Enterprise[2].

# Service Availability

We strive to keep Trello and all associated services fully operational and performant at all times. Occasionally we schedule service outages so that we can upgrade infrastructure components and perform other routine maintenance to keep critical services performing optimally. Infrequently, a situation may arise where emergency maintenance needs to be performed on critical infrastructure or services. Our policies and procedures for handling both planned and unplanned maintenance are below.

## Planned Maintenance

When it is necessary to perform planned maintenance on Trello services, the Trello operations team will perform the work during one of two scheduled weekly maintenance

[1] More about Trello Business Class available at https://trello.com/business-class
[2] More about Trello Enterprise available at https://trello.com/enterprise

windows. We will make reasonable efforts to announce maintenance procedures that could potentially impact users of Trello on the Trello Status Blog[3] and @trellostatus[4] Twitter account at least 24 hours prior to the event, and via an in-app announcement at least 30 minutes prior to the event.

Planned Maintenance Windows:

- Tuesday from 10:00 PM US Eastern Time through Wednesday at 2:00 AM US Eastern Time
- Saturday from 10:00 PM US Eastern Time through Sunday at 2:00 AM US Eastern Time

These windows have been selected with the goal of minimizing service downtime, slowness, or other impact to the people and businesses that rely on Trello.

We do our best to make outages as short as possible. Additionally, our maintenance schedule will frequently be evaluated to ensure that we keep user impact as low as reasonably possible. Should we need to reschedule these windows, the updated schedule will be announced on our Status Blog and Twitter accounts with reasonable advance notice.

### Unplanned Maintenance

Due to unforeseen events, we may have to infrequently perform unplanned maintenance on Trello infrastructure or software components. This maintenance might cause some or all of the Trello services to be inaccessible by our users for a period of time. It is our goal to do this as infrequently as possible. Any unplanned or emergency maintenance will be announced on the Trello Status Blog and in-app with as much advance notice as reasonably possible. As with planned maintenance, we do our best to minimize disruption caused by service outages.

# Security

Many businesses trust Trello to store and manage their important projects, private files, and other sensitive information. We take that trust very seriously and have designed a system intended to protect access to your account and the data you store in Trello. The

[3] Trello Status Blog: http://www.trellostatus.com
[4] @trellostatus Twitter account: https://twitter.com/TrelloStatus

sections below detail our data security policies and procedures that apply to all users of Trello.

## Data Center

Trello production services are hosted on Amazon Web Services' ("AWS") EC2 platform. The physical servers are located in AWS's secure data centers.

From Amazon's documentation:

> *AWS has achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). We undergo annual SOC 1 audits and have been successfully evaluated at the Moderate level for Federal government systems as well as DIACAP Level 2 for DoD systems.*

Further information on the security of AWS EC2 data centers is available directly from Amazon at http://aws.amazon.com/security/.

## Data in Transit

Trello uses industry standard Transport Layer Security ("TLS") to create a secure connection using 128-bit Advanced Encryption Standard ("AES") encryption. This includes all data sent between our web, iOS, and Android apps and the Trello servers.

There is no non-TLS option for connecting to trello.com. All connections are made securely over https.

## Data at Rest

Data drives, on servers holding user data, use full disk, industry-standard AES encryption with a unique encryption key for each server.

For enterprise customers, Trello guarantees that file attachments uploaded after June 3, 2015 will be encrypted at rest using AES encryption. See the section on Trello attachments below for further details.

All backups are encrypted with AES encryption.

## Passwords

All Trello user passwords are stored in salted one-way hashes, never in cleartext. User passwords are not viewable by team administrators or any Trello employees.
Passwords can be reset only by the owner of the account's email address. Password reset emails can be triggered by visiting https://trello.com/forgot/ and submitting the account owner's email address.

## Network Security

Trello production systems are accessible only by members of the Trello operations team who have been properly trained and provided with password-protected digital access keys. Access is further limited to only connections to production systems from authorized IP addresses that are able to securely access the Trello network within the AWS data center.

## Access to User Data

Only authorized and trained members of the Trello operations team have direct access to production systems and user data. Those who do have direct access to data are only permitted to view it in aggregate or for troubleshooting purposes. User data is only viewed by Trello employees for troubleshooting purposes when consent has expressly been provided ahead of time by the account owner or team administrator.

Trained members of the Trello customer support team have case-specific, limited access to user data through restricted access customer support tools. In the event that a support team member needs to view user data, they will first contact the Trello account owner with an email requesting to view their data and including an authorization hyperlink. Only after authorization has been provided by the account owner will members of the support team use their account view tool to view the account owner's data. The account owner can revoke access at any time.

## Trello Attachments

Users of Trello are able to upload files from their computer and attach them to Trello cards. Free users of Trello can attach files that are 10 megabytes or less in size. Trello Gold members and members in Business Class or Enterprise teams can attach files that are up to 250 megabytes in size.

File attachments to Trello cards are stored in Amazon's S3 service. Each attachment is assigned a unique link with an unguessable, cryptographically strong random component, and are only accessible using a secure HTTPS connection. File attachments uploaded after June 3, 2015 are encrypted using Amazon S3 server side 256-bit AES encryption. The encryption, key management, and decryption process is inspected and verified internally by Amazon on a regular basis as part of their existing audit process. At an enterprise customer's request, attachments uploaded prior to June 3, 2015 can be retro-actively encrypted within Amazon S3.

For users who wish to use a different security scheme for attachments, Trello integrates with the following cloud file storage providers:

- Box
- Dropbox
- Google Drive
- OneDrive

When a supported cloud storage provider is used to attach a file to a Trello card, Trello will associate a hyperlink provided by the storage provider with the card. Trello does not store the actual content of the file. The cloud storage provider's own security and permissions system controls view and write access to the attached file.

## Penetration Testing

Trello employs a third party provider to do regular penetration testing. As a general matter, issues that we are made aware of through pen tests or other means are fixed as quickly as reasonably possible. If we ever became aware of an issue where we felt that customer data had been impacted, we would disclose that. It hasn't happened.

# Backups

Data entered into Trello is backed up regularly. All backups are encrypted and stored at multiple offsite locations to ensure that they are available in the unlikely event that a restore is necessary.

Files uploaded to Trello as card attachments are not backed up on the same schedule, and instead rely on Amazon S3's internal redundancy mechanism.
Files associated with Trello cards from a supported cloud storage provider are subject to the storage provider's own backup procedures and policies and are not included in the Trello backup procedures.

## Interval

A rolling live replica of Trello's primary database is constantly being taken on a 1-hour delay. Additionally, a full backup snapshot of the primary database is taken once every 24 hours.

## Encryption

All backups are immediately encrypted with 256-bit AES encryption using GNU Privacy Guard[5] ("GPG") with a password-protected symmetric cipher. Encrypted backups can only be decrypted by members of the Trello operations team who have received training and have been authorized to decrypt the backups.

## Storage

All Trello backups are retained on the following schedule and at the following locations:

- AWS EC2 on a dedicated backup server for two days
- AWS S3 for 7 days
- Google Cloud Storage for 30 days
- AWS Glacier for 90 days

Only authorized members of the Trello operations team have access to the backup locations, so that they are able to monitor the performance of the backup processes, and in the very unlikely event that a restore becomes necessary. After 90 days, the encrypted backup files are destroyed.

## Attachments

Attachments directly uploaded to Trello are handled differently than the primary database backups. To backup file attachments, Trello primarily relies on S3's internal redundancy

[5] GNU Privacy Guard: https://www.gnupg.org/.

mechanism, which Amazon states provides 99.999999999% yearly data durability[6]. Attachments are also backed up to Google Cloud Storage for additional redundancy.

# Data Portability

## Accessibility

Trello board data is available for export by board members in JSON format via the Trello REST API[7]. File attachments can be retrieved individually directly from Amazon S3 using the file's unique hyperlink.

## Automated Export

Trello Business Class and Enterprise editions offer a simplified data export process for all team data and attachments. Each Business Class and Enterprise team includes one-click export of all Boards within the team. Optionally, file attachments uploaded directly to Trello can be included in the export file. Within the export, each board's data is included in both JSON and Comma Separated Values ("CSV") format.

# Business Continuity

The Trello operations team has designed systems to keep the service running even if the underlying infrastructure experiences an outage or other significant issue.

## Replication

Every critical Trello service has a secondary, replicated service running simultaneously with mirrored data in a different AWS availability zone[8] than the primary server. Additionally, each database server has a replicated service running in a third availability zone with data that is mirrored on a one hour delay.

---

[6] More information about Amazon S3's data redundancy can be found at: http://aws.amazon.com/s3/faqs/.

[7] Trello REST API documentation is available at https://trello.com/docs/.

[8] Amazon's EC2 documentation describes availability zones as follows:

> *Amazon EC2 is hosted in multiple locations world-wide. These locations are composed of regions and Availability Zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones. Amazon EC2 provides you the ability to place resources, such as instances, and data in multiple locations. Resources aren't replicated across regions unless you do so specifically.*

Additional information about Amazon EC2 availability zones is available as of the last revision date at http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html.

Because it is important to have reliable access to your business's important projects and data, Trello has been architected to survive a single availability zone outage without significant service interruptions.

### Disaster Recovery

In the unlikely event that two Amazon EC2 availability zones have long-term service interruptions, Trello has been designed to recover with limited service interruption and a maximum of 1 hour of data loss.

In the even more unlikely event that Trello's entire AWS EC2 region is irrecoverably lost, Trello will restore servers using automated configuration systems. In this event, user data would be recovered from backups as quickly as possible, with no more than of 24 hours of data loss.

## Administrator Features

### Google Apps Integration

Businesses that use Google Apps to manage their employee's accounts can connect their Google Apps account to their Trello team that has been upgraded to Trello Business Class or Enterprise. Doing so will enable team administrators to search for new members and add them to their team with a single click.

### Single Sign-On

For enterprise customers, Trello supports account provisioning and authentication via Single Sign-On ("SSO") from SAML v2.0 compliant providers such as OneLogin, Okta, and Microsoft Azure Active Directory.

### Restricted Invitations

Some companies choose to provide Trello access to contractors, freelancers, or consultants. Other businesses want to limit access to their Trello boards to employees only. In either case, administrators of teams that have been upgraded to Trello Business Class or Enterprise can choose to limit invitations to only people with company email addresses.

### Restrict Board Visibility Settings

Many companies use a publicly visible Trello board as a way to communicate with their customers. As an example, our own public board is available at https://trello.com/dev. However, for those businesses who never intend to make one of their Trello boards publicly visible, Trello Business Class and Enterprise enables administrators to configure which board visibility settings can and cannot be used by members of their team.

### Deactivate Members

It is common in IT policies and procedures to revoke an employee's access to key systems and data as soon as they leave the company. However, when these employees had responsibilities on important ongoing projects, it is inconvenient to lose a record of what they were working on just before they left. Trello Business Class and Enterprise team administrators can deactivate a member instead of removing them from the team. Doing so will completely cut off the member's access to the Trello team and all of its boards while maintaining a record of the boards and cards that the employee was a member of prior to being deactivated. Once appropriate transition plans have been made, the employee can be completely removed from the team.

### Read-Only Observers

Sometimes you may want a client, contractor, or someone from another department to view your Trello board, but not have the ability to edit the content. Members of Trello Business Class and Enterprise teams can add Observers to their boards. Observers can see the content of a board, and can optionally be provided with the ability to add comments or vote on cards. However, observers cannot create new cards, move cards, or make other edits to the content of the board.

# Trello Enterprise

## Incidents and Response

A Trello problem impacting a Trello Enterprise customer will be assigned a Severity Level and handled according to the resolutions in Table 1.

*Table 1: Incidents and Response Severity Levels:*

| Level | Description | Resolution | Examples |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Severity 1** | Trello is not available or is unusable. | Work begins within 1 hour from report, temporary resolution within 4 hours, final resolution within 7 hours. | The site is not responding; all text on the site is being translated into elven runes. |
| **Severity 2** | Service or performance is substantially degraded in a way that prevents normal use. | Work begins within 2 hours from report, temporary resolution within 48 hours, final resolution within 14 days. | Search only finds cards with the search terms in the title; Trello cannot be used with the new Firefox version that came out today. |
| **Severity 3** | A service not essential to Trello's main functionality is unavailable or degraded. | Work begins within 72 hours from report, temporary resolution within 7 days, final resolution within 30 days. | Activity indicators are not showing who is active; updates are taking 30 seconds to propagate to other board viewers. |
| **Severity 4** | Minor or cosmetic issues with Trello services, and all feature requests. | Resolution at Trello team's discretion. | Board background images aren't scaling properly; feature request for dependencies between cards. |

In the event of a data breach impacting a client's data, Trello will notify the client as soon as possible within 24 hours after Trello's discovery of the breach.

## Support

The Trello support team assists customers in relaying issues to the development team, finding workarounds for non-critical issues, and helping customers to better understand how to use and implement Trello.

### Support Availability

Support for Trello Enterprise is available during normal business hours, which is Monday through Friday, 9:00 AM to 5:00 PM Eastern Time. The Trello office is closed on the following United States holidays:

- New Year's Day - January 1
- Memorial Day - Last Monday in May
- US Independence Day - July 4
- Labor Day - First Monday in September
- Thanksgiving - Fourth Thursday in November
- Christmas - December 25

When a holiday falls on Saturday, the Trello office will be closed on the preceding Friday. When a holiday falls on Sunday, the Trello office will be closed on the following Monday.

### Support via Email

Trello Enterprise and Business Class[9] customers can email support@trello.com. Trello support will respond within one business day.

### Support via Phone

Trello Enterprise customers may schedule a call directly with Trello support via their account manager or by emailing support@trello.com.

# Termination of Service

## Destruction of Data

On termination of a Trello Enterprise contract, and at the request of the customer, the data belonging to the Trello Enterprise contract's teams will be completely removed from the live production database and all file attachments uploaded directly to Trello will be removed within 30 days. The team's data will remain in encrypted Trello database backups until those backups fall out of the 90-day backup preservation window and are destroyed in accordance with Trello's data retention policy. In the event that a database

[9] This applies to versions of Business Class that are billed per team member. Flat rate Business Class teams may still email support@trello.com, but do not receive priority email support.

restore is necessary within 90 days of a requested data deletion, the Trello operations team will re-delete the data as soon as reasonably possible after the live production system is fully restored.

# Changelog

- 2014-07-28 - First version of document completed.
- 2014-10-28 - Update the *Destruction of Data* section to clarify what happens in the event of a database restore.
- 2014-11-12 - Add *Support* section.
- 2015-06-09 - Add information about encryption at rest.
- 2015-08-03 - Add Business Class customers to “Support via Email” section. Removed outdated process for setting up phone calls with Trello support.
- 2015-10-07 - Change references from ‘organizations’ to ‘teams.’
- 2015-11-20 - Add more details about encryption standards used. Add information about attachment redundancy in Google Cloud Storage. Add the availability of Single Sign-on for Enterprise customers.
- 2017-02-01 - Added information on full disk encryption for data at rest, notification time for a data breach, and updated status blog URL.