Podio by CITRIX

WHITEPAPER

Security overview

podio.com

CITRIX

Podio, a cloud service brought to you by Citrix, provides a secure collaborative work platform for team and project management. Podio features powerful social collaboration tools and customizable workflow apps, plus the ability to seamlessly integrate other cloud services into Podio workspaces. Podio follows the Software as a Service delivery model and does not require any premisebased software deployment. Its interactive, cloud-based work environment empowers teams and individuals to manage workflows and share information through both real-time and asynchronous communication.

Citrix considers the security of your information to be of the highest importance. At Citrix, security is not an afterthought to functionality, but a key element that is designed and built into our systems from the ground up. Security encompasses all aspects of the Podio service, from the software to the facilities to the personnel developing and operating the service. Measures have been undertaken at multiple levels to maintain the privacy and integrity of data managed by Podio. This paper describes some of those measures, including access controls, physical and operational security, data security, and software development lifecycle security.

Protecting the front door

An essential element of information security is the reliable identification and authentication of those accessing the information. Every manner of application, data and network security could be implemented, but if we were not able to reliably identify those accessing the data, we could not achieve the high standard of security that Citrix sets for our services.

For this reason, Podio places great emphasis on user authentication. To begin with, users must be registered using a validated email account, which is associated with an identified organization. No guest or anonymous access to the system is permitted. In addition, numerous techniques are employed to detect and prevent unauthorized account access, such as complex password enforcement, soft and hard account lockout triggered by repeated unsuccessful login attempts, and the logging and continuous monitoring of account probing and other anomalous behavior.

Once a user is authenticated, continued access to the system is dependent upon the presence of a set of security tokens exchanged with the client during the authentication process. These tokens, or session identifiers, are protected using advanced web security mechanisms, including the use of cryptographically strong pseudo-random number generators and session hijacking/fixation countermeasures.

All access to Podio, whether pre- or post-authentication, is permitted only over connections that are secured with Secure Sockets Layer (SSL). Any connection attempt that is not using SSL will be refused. In this way, organizations and users can be assured that all information passed between Podio and the user's browser or mobile app will be safe from would-be eavesdroppers and potential man-in-the middle attacks that rely upon an initial HTTP (unsecured) connection.

In addition to end-user access via a web browser or a Podio mobile app, Podio may be accessed by registered third-party services or applications that are built on the Podio API. Access through the API uses the widely accepted and deployed OAuth2 protocol for authentication and authorization. Beyond the protection provided by SSL/TLS and any native application techniques, every API request is authenticated by the presence of a unique, random access token, securely obtained through OAuth2 using a registered client identifier, client secret, and set of user credentials.

A secure foundation

Although protecting the front door is essential, if the networks and systems that host a service are not themselves secure, the service might still be vulnerable. This, of course, is the reason that Podio is built upon a foundation of network, host and physical security.

Web, application and database servers supporting Podio reside within highly secured worldwide datacenters. Physical access to these datacenters is continuously monitored and restricted to authorized personnel only. The servers themselves are "hardened" to baseline secure configuration standards, and are dedicated to running only those services required to support Podio. Citrix policy requires that servers remain up-to-date with the latest security patches, and undergo periodic reassessment through both internal and independent auditing and penetration testing.

Network access to the systems hosting Podio is strictly controlled through firewalls and other network security devices designed to detect and respond to various attacks, including but not limited to denial-of-service (DoS) attacks originating from the Internet. Backend servers and services are never directly accessible to external systems or personnel. Furthermore, multiple levels of host and network security are employed to ensure that only authorized access is permitted between backend systems, effectively containing any potential internally-leveraged attacks. Access to and activity on systems is centrally logged and continuously monitored for anomalous patterns or behavior.

Safeguarding your data

Once your information has been entered into the Podio system, it is secured with multiple levels of encryption and access controls. Podio is designed to securely allow the efficient sharing of information in a manner that is flexible yet highly visible and easily managed. Data resides in workspaces, which are associated with specific organizations. Only those users explicitly granted access to your information may view or modify it. The design of the system requires that every access request pass through an authorization subsystem that verifies the access rights of the user before allowing the request to proceed.

Not even Podio staff or administrators can access your information, unless you explicitly grant them the right to do so. Unlike some data management systems, Podio does not include the concept of "root" or "superuser" access. This helps to ensure the privacy of your information, even against inadvertent or other internal exposure. Sensitive configuration information, passwords and keys are secured using the latest in cryptographic technology. The Advanced Encryption Standard (AES) is used with a 256-bit key to encrypt sensitive information that must later be available to authorized users in plaintext form. Passwords are secured through a

uniquely salted, one-way (irreversible) password hashing mechanism that ensures protection against exposure even to internal personnel with access to the storage systems and/or encryption keys. Every file uploaded to Podio is encrypted with AES-256 before being transferred to an Amazon Web Services (AWS) S3 repository. Beyond the security safeguards implemented within AWS , the encryption mechanism ensures the privacy of file content. Database backups are encrypted in the same manner as uploaded files.

Secure by design

In addition to the security measures described, the software services that comprise Podio are developed by Citrix using processes that guarantee the integration of security assurance techniques at every stage of the development and deployment lifecycle. Every significant design and architectural decision must undergo a review process known as "threat modeling," in which foreseeable threats to the system are evaluated and measured in light of the proposed design/architectural features. Additionally, code is required to be assessed for security flaws via static analysis, while new and updated systems must be scanned and tested for security weaknesses using industry-leading manual and automated application vulnerability assessment tools.

Availability

All the protection measures in the world will prove meaningless if you cannot access your information or systems when needed. Thus, one of our top priorities in security by design is availability.

With Podio, the continued availability of your information is achieved in several ways. First, the datacenters that host the Podio service incorporate system redundancy throughout in order to ensure resiliency in the face of outages due to failure or attack. Additionally, for the purposes of scalability and reliability, load balancers transparently distribute incoming requests among multiple Citrix servers.

As previously mentioned above, security devices are also in place in every Citrix datacenter to implement countermeasures to denial-of-service (DoS) attacks. To prevent unintended destruction or corruption of information, Podio systems are

backed up hourly and daily, with backups being encrypted and stored at a secure off-site location. Additionally, the Podio interface includes a protection mechanism that requires explicit user acknowledgement before executing any record deletion requests.

Summary

Citrix takes the privacy, security and protection of your data very seriously. We have built our services, including Podio, around this priority. Our security policies and controls align with industry standards, and we review them regularly to ensure continued compliance. Businesses, work teams and individuals can confidently use the Podio service to share information, track projects and manage workflows, knowing that their data is protected by the architecture and policies outlined above.

CITRIX®

Customer Domicile	Contracting Entity	Notice address	Governing law	Governing venue
North, South or Central America, or the Caribbean ("Americas")	Citrix Systems, Inc., 851 West Cypress Creek Rd. Ft. Lauderdale, Florida 33309, U.S.A.	Citrix Systems, Inc., 851 West Cypress Creek Rd., Ft. Lauderdale, Florida 33309, U.S.A.	Florida and controlling United States federal law	Broward County, Florida, U.S.A.
Europe, Middle East or Africa	Citrix Systems International, GmbH Rheinweg 9, CH-8200 Schaffhausen, Switzerland	Citrix Systems International, GmbH Rheinweg 9, CH-8200 Schaffhausen, Switzerland	Switzerland In each case without reference to the conflict of laws principles, and excluding the United Nations Convention on Contracts for the International Sale of Goods	Canton of Zurich