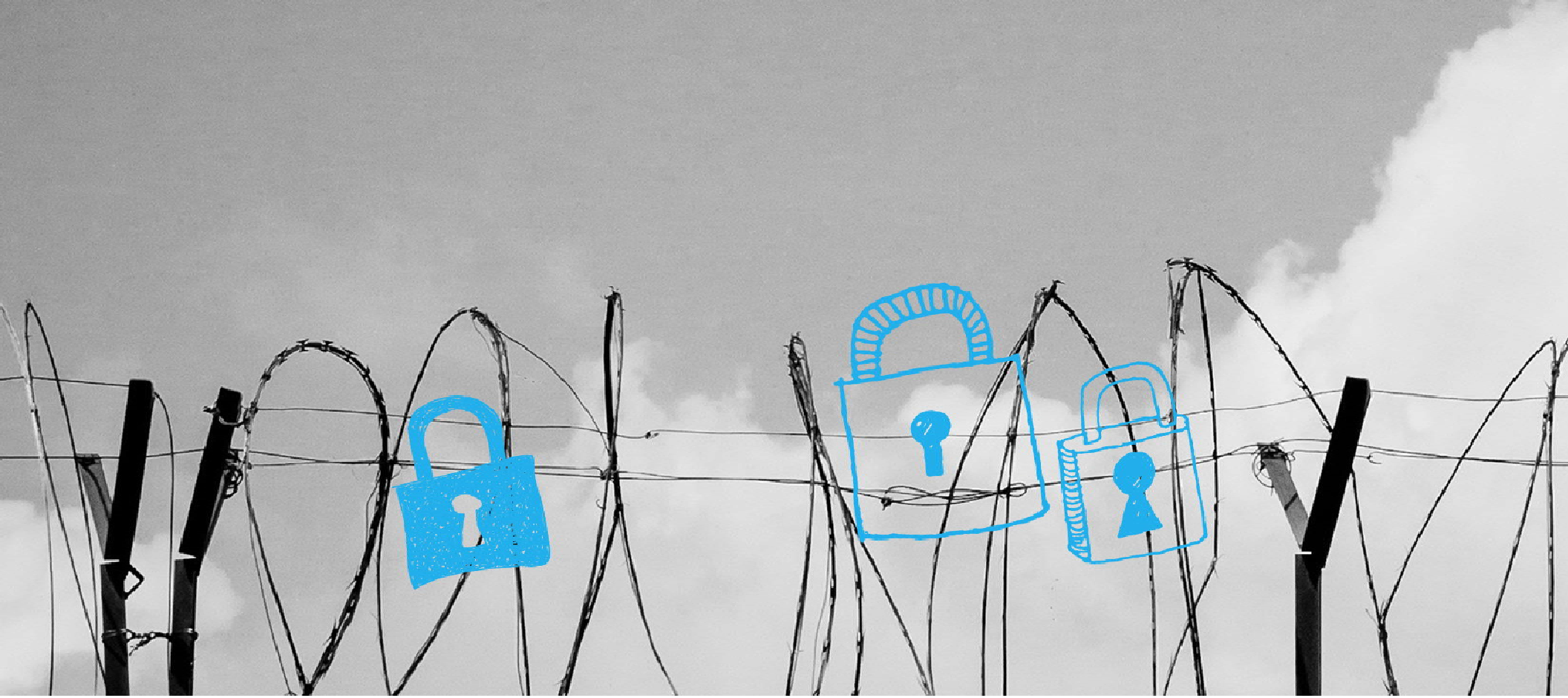


WHITEPAPER

SECURITY + INFRASTRUCTURE

iMeet Central by PGi / Updated January 16, 2023

TABLE OF CONTENTS

INTRODUCTION

The accessibility, security and integrity of your data are integral to the success of your company and the reputation of our business. Because iMeet® Central is delivered as a cloud-based Software-as-a-Service (SaaS) solution, reliability and uptime of our services are of utmost important to your business and our success.

Your data is secure with iMeet Central. The entire platform runs on a proven infrastructure designed to provide maximum security, performance and reliability.

iMeet Central runs inside of Amazon Web Services cloud data centers to provide its customers and partners with state-of-the-art network, server, application and data security to ensure privacy and availability. The AWS cloud infrastructure is the industry standard in cloud infrastructure and services. Customer data is backed up across geographically separated AWS regions to ensure customer data security and integrity in the event of any disaster.

Business these days is global, which is why iMeet Central leverages Amazon Cloud Front content delivery network for global application acceleration. The global AWS Cloud Front footprint boosts application responsiveness and file transfer performance, ensuring you and your collaborators get a great experience, no matter where on the globe you are using the iMeet Central collaboration platform.

We provide the iMeet Central collaboration platform to more than 750,000 users worldwide. Our typical customer is a fast-paced, medium-sized business organization or a team or department within a large Fortune 500 or Global 2000 company. All these organizations, regardless of size, trust and rely on iMeet Central on a daily basis.

KEY SECURITY FEATURES AND ADVANTAGES

Authorized access only

We only allow authorized personnel to access the cloud infrastructure. Authorized personnel must pass criminal and historical background checks and must sign strict non-disclosure agreements (confidentiality agreements) with regards to protecting and accessing customer data. Breaches to the agreements carry severe legal penalties and ramifications. Authorized personnel are required to utilize multi-factor authentication to gain access to both AWS management consoles and cloud infrastructure. Any authorized remote access is solely executed via encrypted communications.

SOC 2 Type II

iMeet Central and Amazon Web Services are SOC 2 Type II compliant. Ask your sales representative for a copy of our latest reports.

SOC 2 Type II is a widely recognized auditing standard. A service auditor's examination performed in accordance with SOC 2 Type II represents that a service organization has been through an in-depth audit of their control objectives and control activities. This audit often includes controls over information technology and related processes. iMeet Central's audits ensure that appropriate processes and controls have been established and that a third party has reviewed these controls over a period of time and found them to
be working effectively. Your company can use the iMeet Central service with complete confidence.

APPLICATION SECURITY

User authentication / login security

- Workspace members (users) are invited by administrators and workspace owners, thus ensuring secure access is restricted to specified users.

- All iMeet Central users create a unique username and password when they create an iMeet Central profile.

- User authentication is controlled via unique and valid username and password combination that is encrypted using a one-way hash. When users submit username and password via this one-way hash to the application, a unique digital signature (or fingerprint) is created, which in turn identifies and authenticates the sender and the contents of the message.

- After the one-way hash secure login, the security model is reapplied with every request and enforced for the entire duration of the session. The security measures are transparent to the user and do not cause any performance drag, latency, or slow down.

- Each additional request is re-verified and if the user's session cannot be authenticated or the user's status on the site has changed (i.e, the user is deleted from the workspace or company by the administrator), the user will not be allowed to access the specified workspace or data.

- iMeet Central does not use "cookies" to store other confidential information and has implemented advanced security methods based on dynamic data and encoded session IDs.

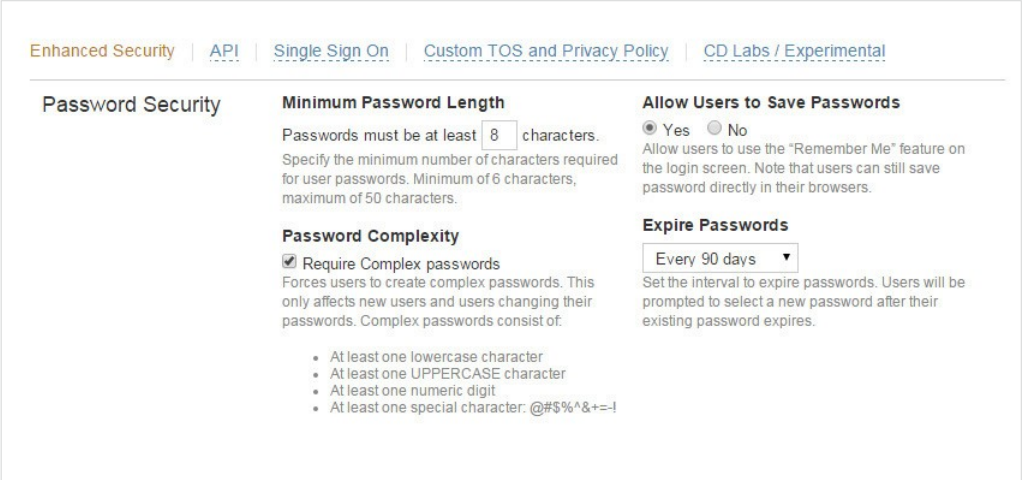
- iMeet Central uses "expiring headers" which enables users with the ability to ensure maximum security after they log out of the application – eliminating the ability for other users to access cached pages in the browser.

Advanced password security options

iMeet Central provides an additional layer of password security by allowing the administrator to adjust a range of password options such as:

- **Minimum password length**
  The administrator can determine what the minimum password length must be for all users within the company. To ensure a minimum level of password security, iMeet Central natively requires a minimum of 6 characters, but can support up to a 50-character minimum password length.

- **Password save option**
  The administrator can determine whether or not to enable the “Remember Me” function at the point of login for all users within the company. This option should be disabled if administrators are concerned about users accessing iMeet Central from public terminals and locations and want to ensure that login credentials are not saved. (Note: Whether or not this feature is enabled, users can still save username and password locally via the web browser.)



- **Password complexity**
  Administrators can require users to use “complex” password credentials. Enabling this feature will require all users to include the following details in passwords:

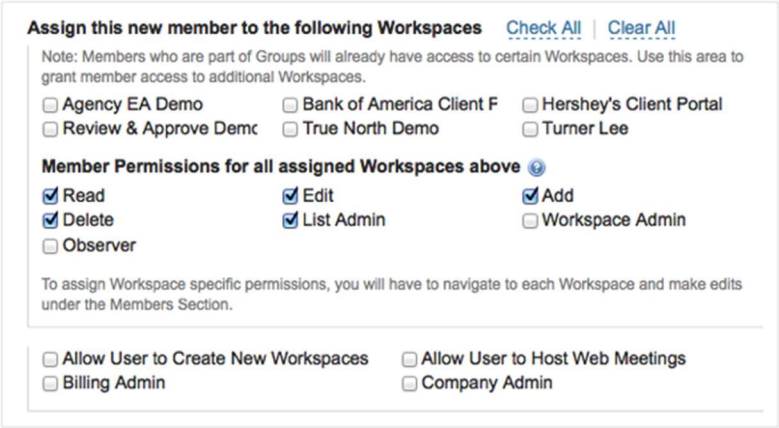
  - At least one lowercase character
  - At least one UPPERCASE character
  - At least one digit (numeral)
  - At least one special character – one of the following characters: @#$%^&+=!

- **Password change frequency**
  Administrators can determine how often user passwords expire, forcing users to create a new password every 30, 60, 90, 180, or 365 days.

- **Single sign-on**
  Large organizations can use their existing Active Directory / LDAP protocols to automatically log in iMeet Central users. iMeet Central Single Sign On is compatible with Security Assertion Markup Language (SAML) v2 and Microsoft’s Active Directory Federation Services (AD FS) 2.0. Additionally, iMeet Central integrates with leading cloud single sign-on providers: Ping Identity, Citrix, Intel, VMware, Okta, OneLogin, and others. Multi-factor authentication support available through integrated SSO providers.

Permissions and rights management

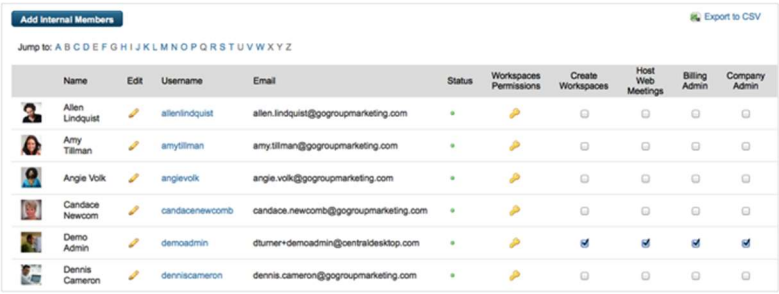
iMeet Central provides customizable permissions and rights management to accommodate a variety of customer needs. User permissions are managed at both the company level and at the workspace level, allowing access to specified workspaces only and allowing the administrator to further restrict user permissions at the workspace level.



Access is controlled at the workspace level and group level for company users.

Company permissions management

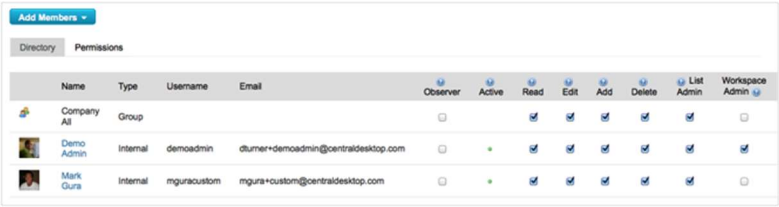
User permissions and access can be managed at the company group level, allowing easy administration of user rights and access to workspaces.



Broad user permissions can be managed at the company level to restrict certain creation and usage rights (including administrative functions).

Workspace permissions management

Granular permissions are managed at the workspace level for users (members) and groups. Permissions such as Read, Edit, Add, Delete and Admin rights are granted on a user-by-user or group-by-group basis at the workspace level.



Granular permission management at the workspace level

TLS ENCRYPTION AND TRUSTED EMAIL DOMAIN SUPPORT

Just as SSL/TLS protects your data in transit to/from your web browser, iMeet Central also uses Transport Layer Security (TLS) encryption protocol to deliver email securely. The TLS encryption and trusted email domain feature allows you to control access and send encrypted emails to trusted users.

Email domains that are listed as trusted domains will receive a TLS-encrypted email with all of the contents of the discussion, comment, or documents available for the user to read.

Email domains that are NOT listed as a trusted email domain will only receive a generic email notification with a direct link to login to iMeet Central.

NOTE: Additional TLS software configuration and setup is required by the company to support TLS encryption on the receiving side of email.

TRUSTED IP ADDRESSES

The trusted IP address feature allows administrators to restrict access to iMeet Central by IP address or IP range. Only listed IP addresses will be allowed access to iMeet Central. This is ideal for organizations that need to restrict access to iMeet Central via a VPN or office location IP address. This feature can be configured at the company level and overridden at the user level.

GLOBAL PERFORMANCE

To assure constant and continuous connectivity to the core Internet backbones, iMeet Central's network infrastructure leverages Amazon Web Services Cloud Front CDN. This ensures global access and reduced latency, no matter where your collaborators are located in the world.

The redundant layers that comprise and support the network infrastructure ensure continuous connectivity. In the event of a bandwidth layer failure, the remaining supporting layers will detect the failure and transfer control in a matter of seconds. This is often described as a "self-healing" or "automated" network. This architecture ensures that any single point of failure prevents network disruption.

The best way to improve web application performance is to get the data closer to the end user. iMeet Central leverages the Amazon Web Services Cloud Front global content delivery network to speed up both application delivery in addition to file upload / download performance.

NETWORK SECURITY

The iMeet Central team has architected a multi-layered approach to secure and defend your data from external attack. We leverage state-of-the-art security methods to prevent unauthorized intrusion by external users attempting to access your data. Our infrastructure proactively deters and monitors for external attacks and unauthorized intrusions.

We employ experienced engineers, system administrators, and IT professionals who pass through rigorous testing, confidentiality agreements, and background checks to secure your data. The iMeet Central team is proactively monitoring and deploying new security measures on a regular basis as appropriate.

iMeet Central's multi-layer network security protection

We believe in the core tenet of security in depth to secure and defend your data from intrusion and attack. Between our servers, which house customer data and the Internet, there are many layers of network security protection:

1. **Amazon Web Services Platform**
   The AWS platform provides all of the core infrastructure that iMeet Central runs on top of. AWS is an industry-leading cloud provider built to satisfy the requirements of the most security-sensitive organizations. Core services such as IP transit, networking, firewall services and server virtualization are fundamental to running a SaaS application. The iMeet Central team has fully evaluated AWS and trusts the data handling processes, compliance and overall security of the platform. **Learn more about AWS Security: https://aws.amazon.com/security/**

2. **Firewall**
   All information and data requests that pass to our servers must pass individual host firewalls. These firewalls place strict limits on ports and protocols and provides the second layer of protection for your data. NAT (Network Address Translation), also known as network or IP masquerading technology, is used in the iMeet Central virtual private cloud to provide an extra layer of security.

3. **Intrusion Detection System (IDS)**
   Passing the firewall, data flows are next scrutinized by the Intrusion Detection System (IDS). The IDS monitors network traffic for malicious activities or policy violations and reports anomalies to the iMeet Central web operations team.

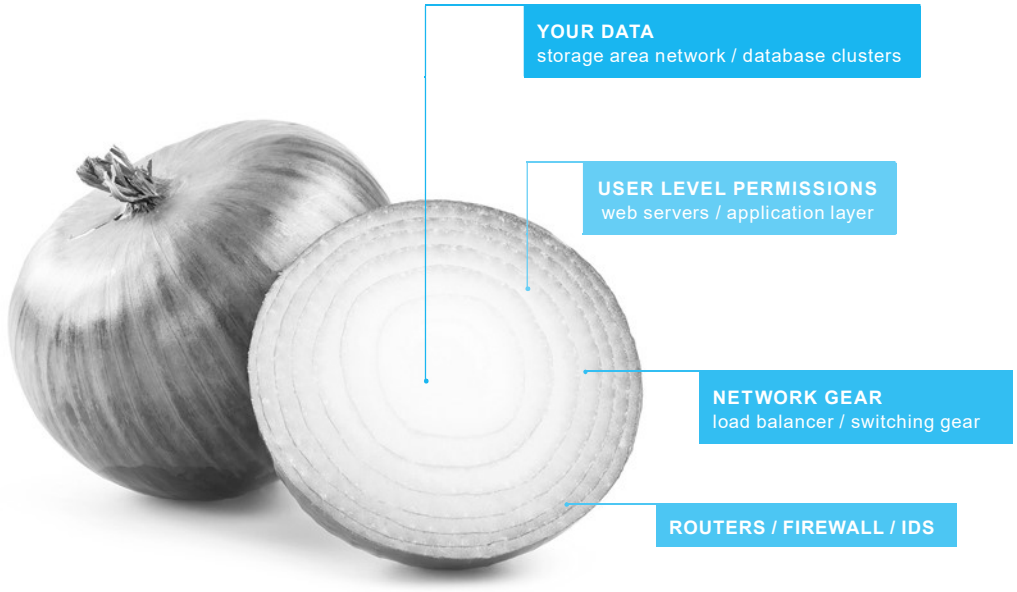
4. **Web server load balancing**
   Web server load balancing, while not strictly a security layer, also provides additional port screening and protocol protection. Web server load balancing can identify common DoS attacks and screen them before reaching the server. It ensures that the URL requests being made are well formed, thus rejecting attempted exploits.

5. **Web/application servers**
   The web/application server layer runs on FreeBSD with Apache as the web servers and iMeet Central as the application server.

   - Apache is configured to minimal configuration specifications required to run our application layer.
   - Application servers are configured to process HTTP requests only.
   - Other non-core Internet protocols and services are disabled.
   - Servers are locked down and secured at the operating system and system directory levels.
   - All non-essential ports and services have been blocked, locked, and disabled.

Security layers

Security is built in from day one with your iMeet Central solution. The entire system, with multiple layers of cloud services, software, and network infrastructure, is designed and optimized to protect your data from intrusion.



Site operations

- Regular operations and system administrator meetings are held to discuss and review near-term and long-term industry-compliant solutions.

- The iMeet Central team proactively monitors industry security warnings, channels, and alerts to uncover new and emerging security risks. iMeet Central engineers act immediately upon the discovery of any security risks or alerts.

- The iMeet Central team proactively scans vendor-specific security channels, including: PHP project, FreeBSD, Linux, plus community-based forums and channels. We also subscribe to all common email virus and bug notification and alerts lists.

Security patches and upgrades

- The iMeet Central team routinely monitors, evaluates, tests, and applies security patches, fixes, updates, and upgrades.

- Any other mission-critical security patches, updates, and upgrades from vendor and community channels are notified and sent to the iMeet Central team and are routinely evaluated, tested, and applied, if applicable, within 24-72 hours of being notified.

DATA INTEGRITY

Millions of data files reside within our customers' iMeet Central workspaces, and thousands of files are added every week. We enlist a variety of methods to assure data integrity, including data protection based on network architecture, as described previously, plus software-enabled SSL data encryption.

Protected data storage

Your data's integrity is protected by numerous layers of state-of-the-art hardware and software security features to prevent hackers or other unauthorized individuals from gaining access to it. With our multiple-layer network security system, your data is safely sequestered well out of harm's way. The following details our approach to "defense-in-depth" security.

- Security model is reapplied with every request and enforced for the entire duration of the session.
- Application security model prevents customer data cross-over and ensures complete customer data segregation and privacy.
- Customer data is segmented from the application layer providing additional security buffers.
- Customer data is encrypted at rest using industry-standard AES algorithms (military-grade tools, NSA-classified encryption, NIST FIPS 197 encryption).

Virus scanning

- iMeet Central servers run the latest version of virus detection software. Our staff's computers are additionally protected by Trend Micro Antivirus.
- Virus scanning software is updated daily.
- Files uploaded to iMeet Central are virus scanned to ensure safe information collaboration.

SSL data encryption

All iMeet Central customers can leverage 256-bit AES High Grade Encryption and SSL (Transport layer security TLS 1.0+) that protects your data using both server authentication and data encryption.

- SSL/TLS encryption technology protects your data from being read during transmission from your computer to iMeet Central servers.
- SSL/TLS encryption software ensures that when the recipient of the transmitted data receives the information, the computer decrypts the information, authenticates the source, and verifies the data integrity.
- SSL/TLS encryption technology leverages digital certificates to verify the identity of the data flow over the internet and allows for encryption and decryption by authorized (authenticated sources).

iMeet Central uses GoDaddy.com Inc. Secure Certificate Authority for its SHA-2 SSL Digital Certificates.

Data backups and restoration

We have implemented rigorous backup procedures to ensure that your data is safely and accurately backed up.

- We maintain a replicated copy of all customer data to a different geographic region in the AWS cloud. This ensures that even if our hosting partner is experiencing catastrophic loss in one geographic area, your data is always safe.
- We execute a daily backup and store data for 90 days.
- Backup procedures include entire data store, databases, and all configurations and code files for all servers.
- All backups are encrypted in transit and at rest using the same level of encryption and protections as live data.
- All backups are rotated into offsite rotation daily.
- The iMeet Central team is able to restore and retrieve data stored for up to 90 days. (Applicable fees will apply.) To initiate a restore request, please contact iMeet Central Support at **support@imeetcentral.com.**
- At any time, workspace administrators can access and download the entire contents of the workspace to give you additional peace of mind so that you can store a back-up of your data.

COMPLETE SYSTEM REDUNDANCY

System redundancy is the key to ensuring consistent and reliable uptime and to eliminating single points of failure. iMeet Central's infrastructure follows an N+1 model to provide full redundancy of all key system components and services. Further, the Amazon Cloud allows us to increase capacity as needed to maintain expected system performance levels.

- Core networking and servers are fully redundant in the AWS cloud.
- Core infrastructure is managed via code. This allows iMeet Central engineers to start up additional servers or even build an entire stack in a different region on demand as needed.
- Multiple load-balanced web servers and application servers are configured to ensure redundancy. If a web server fails, there are multiple web servers available to carry the website traffic and loads without interruption.
- Servers are optimized and configured to accommodate maintenance, software upgrades, server rotation, and configuration without a disruption of service.

COMPREHENSIVE DISASTER RECOVERY PLAN

We have planned for comprehensive disaster recovery and contingencies to protect your data and to provide critical access and business continuity to our applications. Business continuity ensures that you are able to conduct your business in the event of natural disaster or the suspension of services as a result of power or internet connectivity.

Comprehensive disaster recovery ensures the ability to re-establish a working instance of the application in another geographic region if a disaster destroys or renders inoperable the primary AWS region. In the unlikely event of a catastrophic disaster and failure at iMeet Central's primary AWS region, the iMeet Central team has a comprehensive Disaster Recovery Plan in place.

A complete test of this Disaster Recovery Plan is conducted annually and reviewed as a part of our SSAE 16 audit.

Contingencies and plans are in place to ensure that iMeet Central and its customers are up and running with complete application functionality and restored data within 12 hours of the disaster.

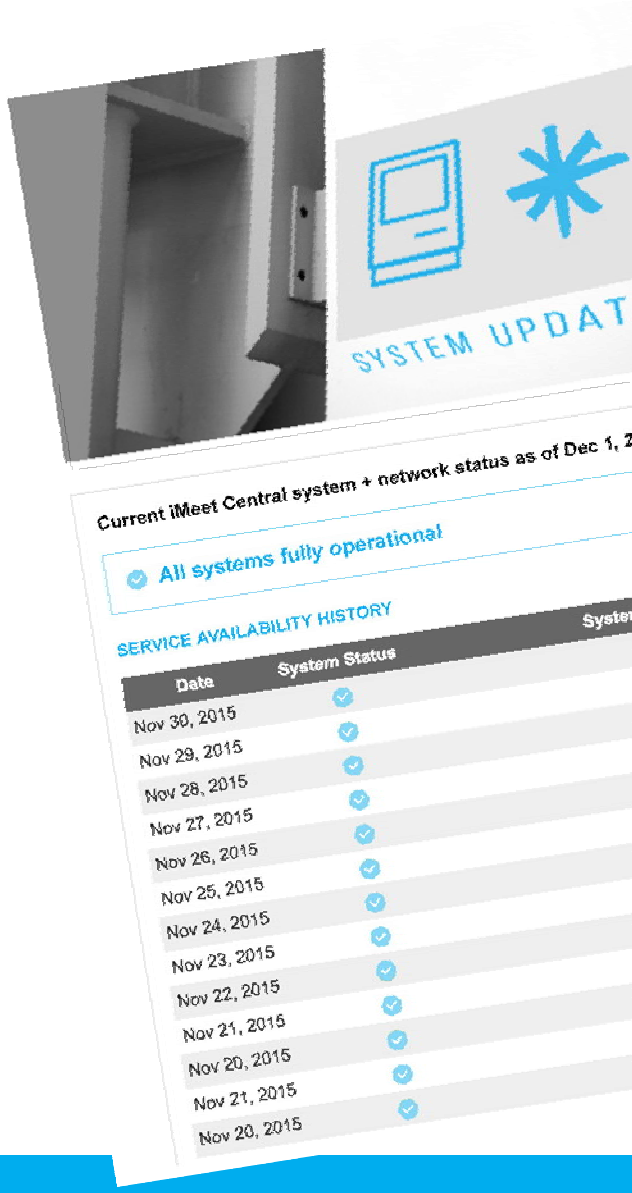
The disaster recovery plan includes guidelines, procedures and clear roles of responsibility and communication amongst partners. The plan ensures timely action and response in such an unlikely event.

- Within 2 hours of notification of the disaster at the primary AWS cloud region, a disaster team is activated and prepared to begin the recovery.
- The secondary region infrastructure is prepared and brought online.
- Key server configuration and customer data is configured to work together.
- iMeet Central customers regain access within 12 hours of the disaster.
- The secondary region is capable of performing all hosting functions in the event of such an emergency or disaster.

UPTIME / HIGH AVAILABILITY

iMeet Central provides industry-leading uptime and service with high availability and uptime.

- The measured uptime for iMeet Central typically exceeds 99.9%. (This is exclusive of scheduled maintenance, which includes server and infrastructure maintenance as well as software updates.)
- Maintenance is typically performed in windows between 12:00 am and 3:00 am Eastern Time on weekends to avoid inconveniencing customers.
- Software update procedures typically require the application to be down for less than 60 seconds at a time. The iMeet Central team schedules software maintenance for weekend mornings (North America time) to ensure minimal customer disruption.
- iMeet Central uses real-time onsite and offsite alerts systems and site monitoring to ensure the availability and performance of distributed IT infrastructures — e.g., servers, operating systems, network infrastructure, AWS services, applications, and application components. Proactive monitoring enables iMeet Central engineers to attack problems immediately before they become critical or emergencies.



SUMMARY:
YOUR DATA IS SECURE AND PROTECTED

iMeet Central provides industry-leading security and protection of your data. Whether you are working from your office, your home, or on the road, you can depend on iMeet Central to be available to you at your critical moments.

The ability to access your data anytime from anywhere ensures that you remain productive, protected, and connected to the information that you need to run your business.

For more information or questions, please contact **Support@imeetcentral.com.**

ABOUT iMEET CENTRAL

iMeet Central helps people work together in ways they never imagined possible.

Our collaboration platform connects people and information in the cloud, making it possible to share files, combine knowledge, inspire ideas, manage projects and more.

More than 750,000 users worldwide use iMeet Central everyday. Key customers include CBS, MLB.com, BBDO, Pizza Hut, Amazon, Sesame Workshop, Pinkberry, the Humane Society of the United States, CareerBuilder, Javelin Marketing Group, Workday and more. iMeet Central is a PGi product.