Instacom
Secure Instant Communication

Designed for Business

Built for organizations to securely unify instant messaging, file storage and file storing with today's popular mobile and desktop systems.

Why Should I Buy Instacom?

As technology evolves, so is the way you are conducting business. With the gaining momentum of mobile computing and the BYOD trend, more and more organizations are forced to embrace and allow employees to use their personal smartphones and tablets for business. What the market is lacking is a platform for employees to communicate and collaborate with clients and co-workers in a secure environment without compromising the organization.

Introducing *Instacom*; one application that works on all devices, including desktops, laptops, smartphones and tablets, regardless of the make or operating system. *Instacom* will allow you to instant message, share and store files on your servers or on your private cloud. No more third party cloud computing where backdoor access and other risks compromise security and privacy. The Centralized Administration Panel gives the you control over user access and activity, with full logging and reporting tools built in for corporate and organization compliance.

You Have Control

Where all your data is on YOUR servers or with your trusted solution provider, not an unknown 3rd party service.

Full archive for accountability and tracking of all conversations, file access and transfers.

All users can be controlled from an easy to use Centralized Administration panel.

User access, groups and contacts can be controlled to fit your needs.

Mobile device users can be instantly removed remotely from the system on demand without physical access to their device.

Secure Instant Messaging

Based on the growing popularity of "texting" as opposed to email, communicate with everyone in your organization openly anywhere at anytime. From office to meetings to home or wherever you happen to be, you can be connected and available.

You can switch seamlessly between devices mid-conversation with all data intact, for example, Desktop to Smartphone to Tablet.

A browser based web client gives you access to the system from any Internet connected device, even if you don't have your computer or mobile device with you.

Store and Share Confidential Data Files

Reduce your FTP costs with the ability to share and store large files.

Access all your stored, sent and received files from your desktop computer and any of today's mobile devices, anywhere in the world.

Invite outside guests or clients into your conversations and file sharing based on granular security and control without compromising system security or client privilege.

Find your files and conversation history with intelligent key word search with context reply.

Secure Across All Devices

| Mobile Devices | Desktops | Browsers |

Control Users

Administrative tools let you control user's time of day, user access and activity. Other aspects of the system are easily defined and set.

File Storage

Control of user file storage access and activities allows for secure file transmission and access to your company data.

Data Encryption

All the data communicated through *Instacom* is protected with AES encryption in addition to SSL. This provides complete security for all conversations and files, ensuring that your valuable information is safe. Each device has its own set of encryption keys that provide increased security, especially for mobile devices.

Full Data And Activity Archive

All your *Instacom* conversations are stored in the system and you can find your data with strong search and reporting tools for compliance and business operations. All transactions for data access, file storage and file sharing are also archived and easily found.

Securely In Your Environment

Flexible implementation options allow you to deploy *Instacom* through your "Private Cloud" with complete security or the system can be deployed in your office, in your existing IT environment, with the same functionality.

Secure Web Browser Access

The *Instacom* web browser client has "Multi Factor Authentication" built in. This means that you need more than just a user name and password to enter the system. You also need a PIN number. Our built in rolling PIN numbers are delivered to the users email at the time of login. Add to this the combination of SSL and rotating AES encryption keys and you can safety use *Instacom* on public computers or in Internet cafes.

Desktop Client Data Access

The *Instacom* desktop clients connect to the *Instacom* server to retrieve data. This eliminates the need to store your sensitive data on local desktop computers within your environment for increased control and security.

Easy BYOD

With the Bring Your Own Device evolution , your users may want to use their own devices for business as well as personal. You can install *Instacom* on their personal devices with the comfort of knowing that the administrative controls of the system can remotely delete all system data, as well as the *Instacom* application, if necessary, keeping all your data safe and secure.

End Point Device Control

With *Instacom* on your end users mobile or remote devices, you still have control of the application and data. *Instacom* is "sandboxed" on mobile devices, meaning the application is segregated to allow removal without affecting anything else on the device. If and when you need to remove a user from *Instacom*, rest assured that the security of the system will keep that user and/or their device(s) from accessing the system and the data.

Device PIN Access

Your installation of *Instacom* on mobile devices is also secured through a 4-digit application PIN code. This code needs to be entered to unlock the application. After a set number of failed attempts to access the system, the data and *Instacom* application will be automatically erased from the device.

Instacom vs. Popular Apps

	Instacom	Lync	Whatsapp	Dropbox
Instant Messaging	Yes	Yes	Yes	No
Mid–Conversation Transition	Yes	Voice calls only	No	No
iPhone	Yes	Yes	Yes	Yes
Android	Yes	Yes	Yes	Yes
Windows Mobile	Yes	Yes	Yes	Yes
Blackberry 10	Yes	No	Yes	Yes
Blackberry 9000 series & below	BB6000 and above	No	BB9000 and above	BB9000 and above
iPad	Yes	Yes	No	Yes
Android Tablets	Yes	Yes	Yes	Yes
OSX	Yes	Yes	Yes	Yes
Windows	Yes	Yes	Yes	Yes
Web Client—2 Factor Authentication	Yes	No	No	No
Controlled Guest Access	Yes	Yes	No	Yes
Secure File Sharing/Transfer	Yes	Yes	No	No
Secure File Storage	Yes (unlimited)	No	No	Yes (limited)
Security Infrastructure	AES + SSL	TLS / MTLS	XMPP	AES + SSL
Privacy Compliance	HIPAA / PCI / SOX	No	No	No
File Transaction History with Search	Yes	No	No	No
Conversation History with Search	Yes	Yes	No	No
Geo-positioning Mapping	Yes	No	No	No
BYOD Friendly with Remote Data Wipe	Yes	No	No	No
Centralized Administrative Controls (not on device)	Yes	Yes	No	No
Software Implementation	In-office servers or by IT service provider	In-office servers or by IT service provider	On Device	On Device
Data Storage	In-office servers or by IT service provider	In-office servers or by IT service provider	None	Amazon S3
Monthly Subscription	$15.00 server/month $4.95 user/month	None	Free	$49.99+ user/month (limited storage)
Software Purchase	$250.00 server $89.00 per user	$3,646.00 server $107.00 per user	Free	None