UnitedDialogue.

Security Overview.

Technical white paper.

Security.

Our first and foremost thought.

At Voris, we deeply care about the security and privacy of our customers.

Voris designed UnitedDialogue platform with security at its core. When we set out to create the best possible social media management platform, we had to build an entirely new architecture for UnitedDialogue from the ground up.

We thought about the security hazards of the cloud software and web applications and established a new approach to security in the design of UnitedDialogue. We developed and incorporated innovative features that tighten security and protect the entire system by default.

Encryption.

Bank level security.

All communications between our server layer applications deployed on our cloud infrastructure and client layer application (UnitedDialogue Dashboard accessed via the browser) are encrypted.

Our security system utilizes Transport Layer Security and several layers of authentication in middle with additional encryptions to assure end-to-end protection of all the data.

Data Security.

Container Architecture.

We use Voris designed Isolated Container Architecture to store data for each UnitedDialogue user.

Whenever a user signs up, the Account Information and Core Associated Data are stored separately with individual configurations profile which is dynamically generated and is associated with security credentials which are a combination of system generated and security information provided by the user.

We also use secured authorization services to monitor all external web links used by UnitedDialogue Core Service for monitoring status and analytics of posts published by the user.

We use redundant storage facilities with built-in fail tolerance and fallbacks for storing all application layer data and we use distributed content delivery networks to deliver the data with high efficiency to our customers from 11 different edge locations.

Product Security.

Global Password Reset.

When our security systems detect any suspicious activities related to unauthorized account usage, we have the process in place to initiate a password reset for all our customers.

Global Account Block.

We have the process in place to automatically block a user when our systems find any unusual activities which may harm the platform.

Strict Email Verification Policies.

We use email verification policies to ensure the identity of the user with a combination of verification locks.

Client Layer Version Expiry System.

We make sure our customers are always using the latest version of our client applications with Version Expiry System. Whenever new versions of the application with critical fixes and security updates are available, we disable support for older versions of the application to make sure all of our customers are protected from new threats.

Voris ActiveSecurity

ActiveSecurity is Voris engineered security monitoring system built on industry standards and open-source projects which can detect threats and vulnerabilities. We have deployed this custom build solution on all our cloud instances which runs UnitedDialogue Core System.

Our team of security experts is working together with the engineering and design team to ensure that our customer's information is completely secure.

We are also into constant dialogue with industry experts, open source communities, security ombudsman of leading companies and banks to ensure the complete coverage of the current trend.

Last updated: September 20 2018