YARA

# 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 YARA platform with security at its core. When we set out to create the best possible event management platform, we had to build an entirely new architecture for YARA from ground up.

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

# Voris Identity.

Voris ID is an unique, common user accounts authentication and authorisation system for all of our products. Voris ID is an isolated entity of its own with independent components which has highest level of security mechanisms in place that are build on top of industry standards. Only Voris designed applications have access to Voris ID services for customer's account level authentication and authorisation purposes.

Voris ID stores all sensitive user related data such as encrypted passwords, personal information of customers which are kept isolated from the application layer (YARA).

There is no public access to Voris ID. Only Voris designed applications can read and modify the data contained within the system by supplying additional configuration profiles and authentication credentials which are dynamically assigned.

Voris ID is build on top of cutting edge security architecture and sophisticated software infrastructure.

# Encryption.

Bank level security.

All communications between our server layer applications deployed on our cloud infrastructure and client layer applications (Including YARA app installed on customers mobile devices and YARA Dashboard accessed via browser) are encrypted.

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

YARA mobile apps use OS specific security encryptions as well as additional methods to safeguard data stored offline on customer devices.

# Data Security.

## Container Architecture.

We use Voris designed Isolated Container Architecture to store data for each YARA Dashboard User or Event Organiser Account information.

Whenever an Event Organiser signs up on YARA Dashboard, the Event Organiser Account Information and Events are stored separately with individual configurations profile which are dynamically generated and are associated with security credentials which is a combination of system generated and security information provided by the user.

The container contains all the encrypted information from Organiser's account details to analytics data generated after events are completed.

We use redundant storage facilities with build-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 6 different edge locations.

# Product Security.

## Global Password Reset.

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

## Global Account Block.

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

## Event Emergency Notifications.

In the event of any emergency situation during an event, YARA can convey the emergency notification to all the delegates.

## Event Data Wipe.

With Emergency Data Wipe, Event Organisers can erase all the event data from every delegate’s device remotely.

## Strict Email Verification Policies.

We use email verification policies to ensure identity of the user with combination of verification locks. We make sure that every email is verified before the complete access to our applications are provided to the users.

## Private and Public Event Types.

Event organisers can set security type for an event. With Private Event Security type, organiser can enable restrictions to keep event completely private.

## Flagging System.

YARA applications (both mobile apps and web dashboard) are built in such a way that they can recognise all the abusive words and can block the users from posting them.

## Client Layer Version Expiry System.

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

# Mobile App Security.

## Encrypted Offline Database.

All the data stored on the devices and kept offline are encrypted using OS specific security methods with additional safeguards.

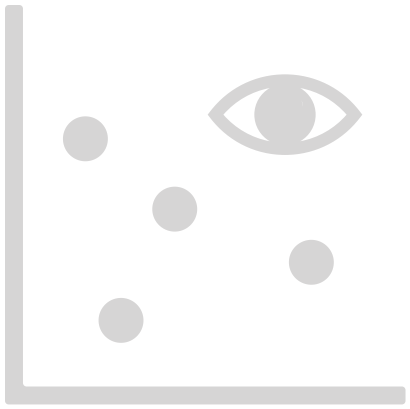
## Encrypted Communications.

All the communication between YARA mobile apps and YARA Core System which are hosted on cloud infrastructure are encrypted by default.

## Credentials Usage.

We never store the user credentials such as usernames or passwords on devices. They are discarded after the user is signed in to the application. We use a different set of 6 unique credentials to authenticate each request made between Mobile Apps and Core System after a successful login.

# 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 YARA Core System.

Our team of security experts are working together with the engineering and design team to ensure that our customer's information are 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: June 3 2018**