Commonly Asked Questions about TAP App Security

Q1: What does "private network" mean, and will it be cellular, 4g or on a company's network?

Private network refers to *closed networks* meaning where the interconnection of users in the specific organization can communicate. In our case "private network" does not mean the cellular network or any other means of you connecting to the internet. We create closed (or private networks) for each organization (e.g. Business, Workplace, Construction Site, Police, Fire, EMS, Government Facility, etc.) that requires access codes. For example, employees at a specific location (i.e. Building A) will be on the same network and can only log into the network by using a special code for their specific location. Tap App is not designed for the general public but rather for organizational leaders (decision-makers) and their employees. It operates off cloud servers, and works on wireless, cellular, and 4G.

Q2: What happens if during a real emergency the app fails to activate due to either an error on the phone/device or an error in the "private network?"

One of the primary goals of the TAP App Security system is to enhance communications during emergencies. If there is a problem with the system or someone's cellular phone that is using the system, other means of communication should be utilized (e.g. radio, telephone, PA system, etc.). As with any technology, there is always the possibility of system failures. Although rare, it must still be a consideration. Tap App runs off cloud based servers that are scattered around the United States and is extremely reliable. If a bug occurs in the system then it would need to be fixed as soon as possible (obviously after an emergency). We are strong proponents of redundancy in communication when it comes to emergency management. We want organizations to use all available methods to communicate. TAP App Security should be an addition to, not a replacement of other modes of communication.

Q3: Would this app have to be running all the time, and what happens when someone's mobile device/phone runs out of power?

The system is purposely designed as a horizontal communication system. There will be multiple users on the network so if one link of the system (or user's device/phone) is not working, the system is still useful to the other members assuming their devices are charged and working. It would be unlikely if every person's communication device was down at the same time. If that occurs then the scope of the emergency is so severe that it would likely impact all other forms of communication as well. We hope that never happens. Tap App is designed as a multi-stakeholder collaboration tool with numerous users with numerous different devices. As mentioned above, this is an "addition to" not a replacement of. The app will not put extra strain on smart device's batteries because it does not "run" until it is activated by a user within the network. Tap App also sends email messages and works on computers and laptops.

Q4: What kind of contractual commitment is required for purchasing the app?

There is normally a 12-month licensing commitment for usage of the app. Renewal after the first year is optional. We do consider temporary trial periods (e.g. 3 months or 6 months) for a reduced cost on a case-by-case basis. However, our pricing points are low enough that a 12 month commitment is very attractive. Clients are free to discontinue service if they are not pleased with the product.

Q5: How do clients stay proficient when it comes to using the app? What if there are no emergencies that require the app to be used?

We hope that your organization does not have to use the app for real emergencies often. Everyone prefers to prevent incidents before they occur. That said, we want to ensure that our clients are well-prepared to use the app if prevention fails or if there is a natural hazard or human-caused threat. To help clients stay current with using the app, we provide free quarterly webinar trainings where the app will be tested. Tap App also includes a "Drill Mode" feature that allows clients to use the app for training (tabletop or real exercises) without disrupting normal business operations. Although Tap App is extremely simple to use and practical for workplace environments, we provide continuous support to clients so they remain familiar with the system and stay vigilant at maintaining safer and more secure workplace environments.

Q6: Who is supplying technical support for the app?

Technical support is provided in two ways. 1) We provide our clients with 24/7 Tech Support. If a problem occurs with the app, users can report the issue by completing a digital ticket on our website and it will be fixed by our team of engineers and developers. Most issues will be fixed with a few hours after we're notified. 2) For minor technical issues, such as an employee forgetting their password, or setting the app to "drill mode" so it can be used for training, or printing out after-action reports, we establish Organizational Administrators at organizations. These individuals (usually managerial level or above) will have full access to the back-end of their system through the web version of the app. We provide this level of access to clients so they have complete oversight and control over their own system. Extra training is provided to organizational administrators. TAP App does not create extra work for people at organizations but rather assists leaders to carry out their protective roles and reduce risk at work.

Q7: Can the app access personal information from cell phones/mobile devices?

The TAP App Security system does not access personal information from your cell phone/mobile device. The main features of the app are internal to the Tap App system. Such features allow users to take attendance, report missing persons, report persons found, send priority messages (including digital images), access emergency plans, maps, and the Incident Command System. There might be personal phone numbers and emails uploaded into the app for the Incident Command System feature. However, users would have to voluntarily agree (give permission) to have that information in the app. All federal and state privacy laws are adhered to. Additionally, as part of the Term Sheet, is a "confidentiality agreement" to assure clients that personal information will not be disclosed and will be well protected.

Q8: What sort of cyber protections are in place for the app?

The app is hosted on secure cloud servers. We use Digital Ocean in New York City and Amazon Web Services throughout the United States. Digital Ocean and Amazon Web Services are trusted hosting partners for top American companies. Back-up servers are scattered all across the United States. Access to the data is restricted by username and password credentials under supervision of local administrators and super-admins. The security of the connection is controlled by the 256-bit token that is given to the device during registration. Additional information can be found at: www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers. The same cybersecurity used by banks in the U.S. is used by Tap App.