// THE WICKR PRO DIFFERENCE

SECURE // EPHEMERAL // AVAILABLE

WickrPro is a vetted, simple to use platform built by an expert security team to protect high-value sensitive communications & files. Messages, large files, calls and video conference. All end-to-end encrypted. All ephemeral.

User data is encrypted on the sender's device and only the recipient can access it. Nobody else has the keys to decrypt your messages or documents, including Wickr. Your communications are not stored on a server. You control how long each message and file lives. Always.

"Government and private enterprises are constantly targeted by state and non-state actors. From elections to highly sensitive diplomatic and business negotiations, securing data is undeniably mission critical. Wickr's end-to-end encryption and data minimization approach finally enable organizations to insulate high-target communications from diverse and persistent threats."

— Ambassador Joseph DeTrani, Former U.S. Special Envoy and Former Dir National Counterproliferation Center

WICKR PRO FEATURES AND CAPABILITIES

1:1 AND SMALL-GROUP MESSAGING
End-To-End Encrypted Ephemeral Conversations

SECURE ROOMS & CROSS-NETWORK COMMUNICATION
Invite Teams To Communicate & Collaborate

FILE TRANSFER
End-To-End Encrypted Ephemeral Files Up To 5Gb

VOICE, VIDEO & SCREEN SHARE
End-To-End Encrypted Calls & Video Conference

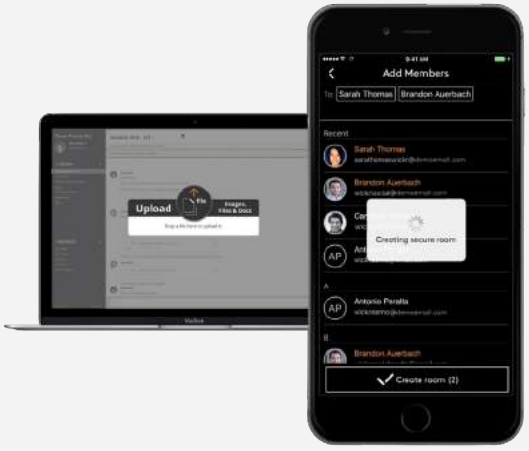
PROVISIONING & ADMIN CONTROLS
Easy On-Boarding // Secure Private Network Deployment In Minutes

ADVANCED LAYERED SECURITY
No Third Party Including Wickr Can Access User Messages

CONFIGURABLE EPHEMERALITY
Messages Are Not Accessible Beyond Set Expiration Or Burn-On-Read Time

PERFECT FORWARD & BACKWARD SECRECY
New Key Generated For Every Message

WICKR PRO FOR POLITICS



With today's state of end-point security, it is essential to run sensitive operations on a vetted secure channel, minimizing a chance for discovery by an adversary.

WickrPro is built as a hardened security environment to mitigate these risks, mirroring the expectations of a face-to-face meeting among trusted parties.

Visit www.wickr.com for more information

POLITICAL BEST PRACTICES FOR SECURE COMMUNICATION:

- For most effective use, set your own internal organizational rules & protocols to ensure all valuable conversations take place on a secure ephemeral channel.
- No discussion about Members, candidates or prospective candidates on email or unencrypted apps.
- No self or opposition research books should be distributed via email or unencrypted apps — internally or externally.
- No surveys or polling memos/decks should be distributed via email or unencrypted apps — internally or externally.
- No conversations about a candidate or elected official should take place on email or unencrypted apps.
- No donor information should be shared via email or unencrypted apps.

Randy Brumfield
VP Corporate Development & Customer Success
Cell: 408-621-2986 // Email & WickrPro: rbrumfield@wickr.com