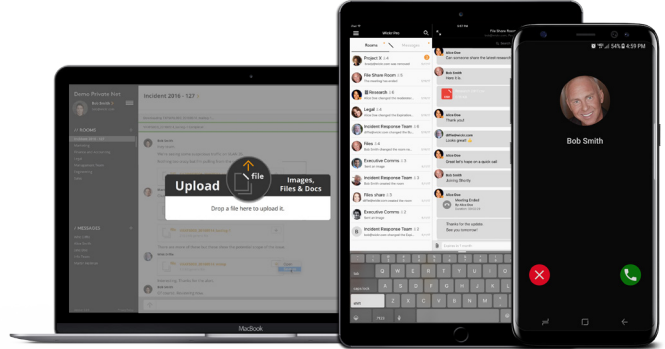


# // THE WICKR PRO DIFFERENCE

## 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.



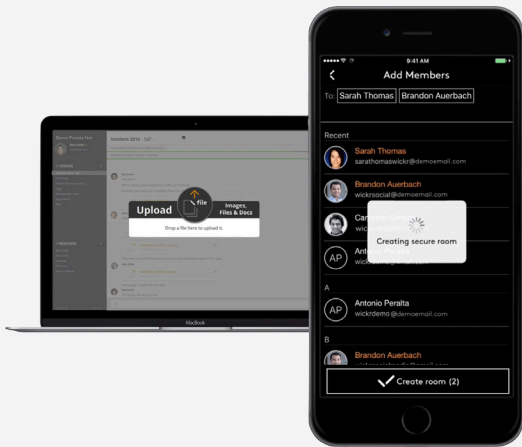
“Wickr allows companies and organizations to bring the security and privacy of a face-to-face conversation to digital collaboration.”

— Thomas Tull, CEO of Tull Investment Group & Founder of Legendary Entertainment

## 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](http://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.



Audra Grassia  
Political & Government Lead, Privacy Communications  
Cell: 617-447-4934 // Email & WickrPro: [agrassia@wickr.com](mailto:agrassia@wickr.com) // WickrMe: @agrassia