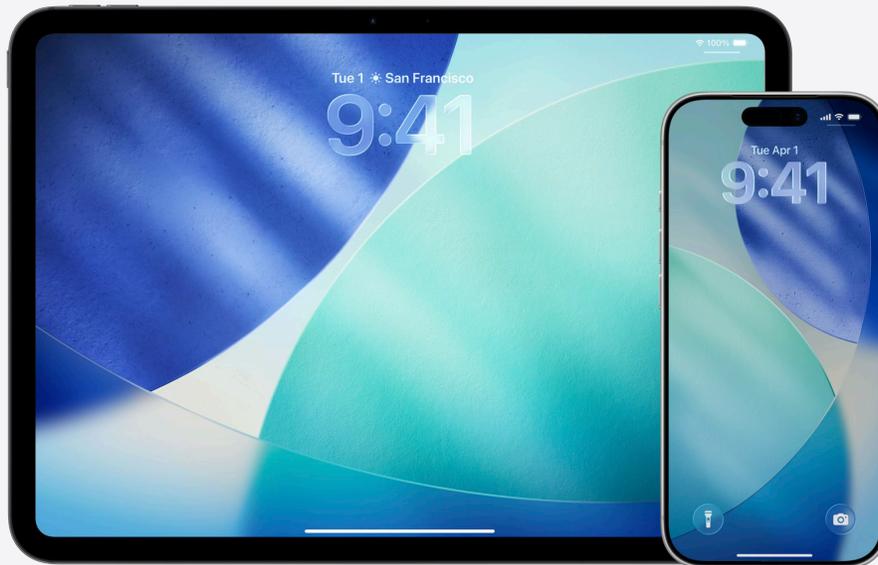# iPhone and iPad for NATO classified use

Apple devices are as secure as they are easy to use. Securely access Mail, Calendar, and Contacts data at NATO RESTRICTED level using apps built for iPhone and iPad with the Indigo approval.

✓ **Indigo approval for iPhone and iPad.** Users can use the Mail, Contacts, and Calendar apps on iOS and iPadOS for NATO Restricted level data. Indigo doesn't require any special additional software or settings beyond managing and supervising devices using a device management service.

✓ **Apple silicon.** Apple silicon works seamlessly with iOS and iPadOS to deliver advanced security and privacy features to keep your operating system and data safe. And Apple silicon features Secure Enclave, which encrypts and protects user and biometric data and enforces passcode policies.

✓ **Touch ID and Face ID.** Touch ID and Face ID give you a fast, easy, and secure way to unlock devices, open protected files, and retrieve passkeys at a touch or a glance. So you won't waste time looking up forgotten passwords.

✓ **Memory Integrity Enforcement (MIE).** MIE combines Apple silicon hardware and advanced OS security to deliver industry-first, always-on memory safety for devices with A19 and M5 processors— without impacting performance. It is the biggest memory safety advance in consumer OS history.

✓ **VPN and secure networking.** Apple devices support virtual private networks (VPNs) out of the box, to encrypt and protect critical data. iOS, and iPadOS work with the industry-standard networks you already use, like IKEv2, Cisco IPsec, and L2TP over IPsec.

For more information on how Apple devices can be used by your organization, visit apple.com/government.