Device checklist: Requirements for using passkeys

Criterion	Explanation	Fulfilled? (Yes/No)	Notes / Measures
Current operating system	Windows 10/11, macOS 13+, iOS 16+, Android 9+		Upgrade outdated OS versions if necessary
TPM/Secure Enclave available	TPM 2.0 for Windows, Secure Enclave for Apple		Check BIOS/UEFI, activate if necessary
Device lock enabled	PIN, fingerprint, or facial recognition		Requirements for platform authenticators
Compatible browser installed	Chrome, Edge, Safari, Firefox (current Version)		WebAuthn support required
Biometric sensor available	Fingerprint sensor or camera for Face ID / Windows Hello		Alternatively: PIN login as a fallback
MDM or device management available	Central management (e.g., Intune, JAMF, VMware Workspace ONE)		Important for policy control and recovery
Synchronization with cloud service allowed (optional)	iCloud, Google Password Manager		Enable or disable depending on compliance requirements
External authenticators can be connected (optional)	USB, NFC, or Bluetooth-enabled devices		For hybrid or high-security applications