

// DESKTOP HARDENING

MACBOOK & IMAC HARDENING GUIDE

A step-by-step configuration reference for reducing your device's digital exposure. Each setting reflects best practices for principals, family members, and anyone in a high-visibility role.

Note: If an app has access to contacts, photos, microphone, or camera and shouldn't — remove access immediately.

// PRIVACY & SECURITY 01

SETTINGS › PRIVACY & SECURITY

 Location services › App access CONFIRM APPS

 Significant locations TURN OFF AND CLEAR HISTORY

 Full disk access CONFIRM NOTHING HAS ACCESS

 Contacts access CONFIRM APPS

 Microphone access CONFIRM APPS

 Photos access CONFIRM APPS

 Camera access
Remove access for any app that shouldn't have it CONFIRM APPS

ANALYTICS & IMPROVEMENTS

 Share Mac analytics TURN OFF

 Improve Siri & Dictation TURN OFF

 Share with app developers TURN OFF

APPLE ADVERTISING

 Apple advertising TURN ALL OFF
// NETWORK & USERS 02

SETTINGS › NETWORK

 Firewall TURN ON

SETTINGS › USERS & GROUPS

 Guest user TURN OFF
// FILEVAULT & TOUCH ID 03

SETTINGS › PRIVACY & SECURITY › FILEVAULT

 FileVault TURN ON

SETTINGS › TOUCH ID & PASSWORD

 Touch ID options CONFIRM CHOICES FOR TOUCH ID
// APPLE ID & ICLOUD 04

SETTINGS › [YOUR NAME]

 Sign-in & security › Trusted phone number REVIEW

 Two-factor authentication TURN ON

 Devices on Apple account REMOVE UNKNOWN/ OLD DEVICES

 iCloud backup TURN ON

 Private relay (iCloud+) TURN ON

 Advanced data protection (iCloud+) TURN ON

 Data access on iCloud.com TURN ON

BACKGROUND SECURITY

 Background security improvements
Automatically install TURN ON