SETUP GUIDE

macOS Security Setup Guide for Web3 Teams

A self-service baseline that works without MDM

Prepared for	Web3 team members	Classification	Internal
Prepared by	Oak Security	Date	2026-06-17

Oak Security GmbH

1. What This Guide Is For

This guide is for anyone in a Web3 team who uses a Mac for work, whether you are a developer, an operator, or in a non-technical role. Most of the setup is designed to work **without Mobile Device Management (MDM)**: you should be able to apply the baseline yourself, without turning your laptop into a centrally managed device. Section 2 describes lightweight MDM-style options for teams that decide they want them.

The aim is not to make every Mac identical. It is to make sure a normal laptop problem, such as a bad browser extension, a suspicious download, a stolen session, or an unlocked screen, does not turn into a company-wide incident.

> **NOTE**
>
> **Baseline rule:** any Mac used for work should be encrypted, updated, locked when unattended, separated from risky personal browsing, and kept free of unnecessary extensions and local secrets.

For the most sensitive work, such as production administration, cloud/KMS access, DNS or registrar changes, treasury signing, source-control organization administration, and release approvals, a dedicated hardened work device is still the better option.

2. Lightweight MDM Options for Company Macs

This guide is deliberately self-service friendly. It does not require MDM, and it should not be used as a reason to manage personal devices without a clear company decision.

If your team starts issuing company-owned Macs, the same baseline can move from "please configure this yourself" to "the company enforces this by default." That does not need to be heavyweight. A small team can start by managing the devices of critical operators first.

Practical Options

Option	Best Fit	Notes
Apple Business Essentials	Small Apple-first team that wants Apple's own lightweight device management, support, and storage bundle.	Good low-friction starting point for company-owned Apple devices, subject to regional availability and licensing.
Apple Business Manager plus MDM	Team that wants automated enrollment plus an MDM such as Jamf Now, Mosyle, Kandji, or Intune.	Apple Business Manager handles device assignment and enrollment, but it is not by itself the full MDM control plane.
Jamf Now / Mosyle / Kandji	Small team that wants a simple Apple-focused MDM without a large enterprise deployment.	Useful for inventory, profiles, app deployment, FileVault enablement, and recovery-key escrow.

Configuration Profile (.mobileconfig) Option

For a distributed team without a full MDM, a signed `.mobileconfig` configuration profile is a relatively simple way to distribute consistent macOS settings. It sits between self-configuration and fully managed devices.

A profile can bundle settings such as Wi-Fi or VPN configuration, certificates, restrictions, and other Apple configuration payloads. Users still install it themselves, and the team still needs a clear process for versioning, signing, distribution, and removal.

Treat `.mobileconfig` as standardization, not full management. It does not replace MDM for inventory, remote wipe, FileVault recovery-key escrow, forced updates, app deployment, or reliable offboarding.

A Sensible First MDM Rollout

Start with company-owned devices for high-risk users only:

- head of engineering;
- production administrators;
- release owners;
- treasury signers;
- DNS, registrar, source-control organization, hosting, and cloud/KMS administrators.

For those devices, enforce only the controls that reduce the most risk:

- FileVault on, with recovery key escrowed;
- automatic macOS update checks;
- screen lock and password requirement;
- firewall on;
- unused sharing services off;
- basic app and extension inventory;
- a remote wipe or rebuild path for lost or compromised devices;
- clear ownership and offboarding.

Keep the self-check below for personal devices. Use MDM for company Macs where the company has a legitimate need to enforce and recover the device.

3. Quick Setup Checklist

These are the settings every work Mac should have before it is used for work.

macOS Settings

Setting	What To Do	Where To Check
Updates	Install pending macOS updates. Turn on automatic update checks.	System Settings > General > Software Update
FileVault	Turn on full-disk encryption. Store the recovery key in your password manager.	System Settings > Privacy & Security > FileVault
Screen lock	Require a password immediately after sleep or screen saver starts. Use a timeout of 5 minutes or less.	System Settings > Lock Screen
Firewall	Turn on the macOS firewall. Enable stealth mode if it does not break your normal work.	System Settings > Network > Firewall
Sharing	Turn off sharing services you do not use. Pay special attention to Remote Login, Screen Sharing, File Sharing, Remote Management, Bluetooth Sharing, and Internet Sharing.	System Settings > General > Sharing

Work Separation

Area	What To Do
Browser profile	Create a dedicated browser profile for work. Use it for email/workspace, source control, chat, docs, hosting, cloud, registrar access, and the password manager.
Personal browsing	Keep personal browsing, airdrops, trading, wallet

	testing, and random web apps out of the work profile.
Wallet activity	Do not mix personal wallet activity with production, admin, or company SaaS sessions. Use a separate profile or browser.
Extensions	Remove extensions you do not need. Do not install wallet, coupon, scraping, AI helper, or unknown extensions in the work profile.

Credentials, Keychain, and Local Data

Area	What To Do
Passwords	Store work credentials in the team-approved password manager. Do not store them in Notes, screenshots, chat, shell history, or local files.
Apple Passwords	Apple Passwords and iCloud Keychain are fine for personal credentials. For work credentials, use them only when the team accepts that the credential may sync to your personal Apple devices.
MFA	Prefer passkeys where supported. Use hardware security keys for critical accounts where possible.
Local secrets	Check Downloads, Desktop, screenshots, Notes, shell history, dotfiles, `.env` files, SSH keys, API keys, and access tokens. Remove anything that should not be local.
SSH keys	Use a separate SSH key for work. Do not sync private SSH keys through iCloud, Dropbox, Google Drive, or chat.
Backups	Use encrypted backups. Do not back up seed phrases, plaintext secrets, private keys, or sensitive screenshots into uncontrolled personal cloud storage.

4. Password Managers, Passkeys, and Hardware Keys

Use different storage models for different risk levels. A synced password manager is a good default for normal work credentials. It is not the same thing as a hardware-bound key.

Storage Model	Use For	Caveat
Team-approved password manager	Normal work passwords, recovery codes, low-risk SaaS credentials, and shared team credentials.	Good organizational control, but synced vault secrets are still usable if the vault and endpoint are compromised.
Apple Passwords / iCloud Keychain	Personal credentials, and low-risk work credentials if the team accepts the sync model.	Credentials and passkeys may sync to personal Apple devices outside company visibility.
Hardware security key / hardware-backed passkey	Critical accounts such as email/workspace, source-control admin, cloud, hosting, registrar, and password-manager admin.	Less convenient, but stronger because the private key is bound to a physical authenticator.
Hardware-backed SSH key	Production or sensitive repository and infrastructure access.	Requires setup discipline and backup keys, but avoids storing reusable private keys in files or synced vaults.

Practical Policy

- Use the team-approved password manager for normal work credentials.
- Use hardware security keys or hardware-backed passkeys for critical accounts.
- Do not treat synced password-manager passkeys as equivalent to hardware-bound credentials.
- Do not store SSH private keys, production secrets, API tokens, wallet seed phrases, or critical recovery codes in Apple Passwords, iCloud Keychain, Notes, screenshots, or local files.

- If Apple Passwords or iCloud Keychain holds a work credential, understand that every synced Apple device becomes part of the access surface.

5. Apple Passwords, Keychain, and iCloud

Apple Passwords and iCloud Keychain are convenient and generally well-designed for personal use. The work concern is not that Apple Keychain is weak. It is that Apple Keychain can sync work credentials and passkeys into personal Apple devices that the company does not know about and cannot clean up during offboarding or an incident.

Recommended Approach

Topic	Guidance
Apple Passwords app	Use it for personal credentials. For work credentials, use the team-approved password manager by default.
iCloud Keychain sync	Treat iCloud Keychain as a sync path to every device on the same Apple Account. If a work credential or passkey is stored there, every synced device becomes part of the access surface.
Passkeys	Passkeys are good, but synced passkeys are still credentials. For critical accounts, prefer hardware security keys or hardware-backed passkeys.
Local macOS Keychain	It is normal for apps and the OS to store some tokens in Keychain. Do not manually store production secrets, seed phrases, API keys, KMS material, recovery keys, or SSH private keys there for convenience.
iCloud Drive	Do not keep work secrets or confidential files in personal iCloud Drive, including Desktop and Documents sync. Use the approved company storage location.

If you use Apple Passwords or iCloud Keychain for any work credential, make sure:

- Your Apple Account has a strong unique password and MFA.

- No one else uses your Apple Account.
- Every synced device is encrypted, updated, and locked.
- Old or unused Apple devices have been removed from the Apple Account.
- You understand that incident cleanup may require reviewing every synced Apple device, not only the Mac used for work.

6. SSH Keys and Developer Credentials

SSH keys, access tokens, cloud credentials, and API keys deserve separate handling. They are often more useful to an attacker than a normal website password.

Baseline Rules

- Use a separate SSH key for work.
- Prefer modern key types such as ed25519 unless a service requires something else.
- Protect file-based private keys with a passphrase.
- For production or sensitive infrastructure access, prefer hardware-backed SSH keys.
- Do not store private keys in iCloud Drive, Dropbox, Google Drive, chat, docs, screenshots, or email.
- Do not share private keys. Share public keys only.
- Do not reuse personal SSH keys for work infrastructure or repositories.
- Avoid SSH agent forwarding unless there is a clear need.
- Remove old keys from source-control accounts and servers when they are no longer needed.
- Rotate SSH keys and tokens after suspicious device activity.

Suggested Developer Self-Check

Check	Pass Condition
Separate key	Work uses a dedicated SSH key.
Private key storage	Private key is not stored in any synced folder or chat history.
Passphrase	File-based private key has a passphrase.
Hardware-backed key	Critical infrastructure access uses a hardware-backed SSH key where practical.
Source-control keys	Your source-control account has no stale or unknown SSH keys.

Tokens	Access tokens and API keys have clear purpose, limited scope, and expiry where possible.

7. The Recommended Setup Flow

Step 1: Update macOS

Open **System Settings > General > Software Update**. Install anything pending and turn on automatic update checks.

Do not sit on security updates for weeks. If an update has to be delayed because it may break a tool, say so in the team channel and set a date to revisit it.

Step 2: Turn On FileVault

Open **System Settings > Privacy & Security > FileVault** and enable FileVault.

Save the recovery key in your password manager. Do not save it as a screenshot, local note, chat message, or file on the same laptop. A recovery key stored on the device it unlocks provides no recovery if that device is lost or encrypted.

Step 3: Lock the Device Properly

Open **System Settings > Lock Screen**.

- Require the password immediately after sleep or screen saver starts.
- Set the screen saver or display timeout to 5 minutes or less.
- Lock the screen manually before stepping away.

Endpoint security is mostly about making the easy mistakes harder to make.

Step 4: Enable the Firewall and Turn Off Sharing

Open **System Settings > Network > Firewall** and turn the firewall on.

Then open **System Settings > General > Sharing** and turn off anything you do not actively use. Most people should not have these enabled all the time:

- Remote Login
- Screen Sharing
- File Sharing

- Remote Management
- Bluetooth Sharing
- Internet Sharing

If you need one of these for a real workflow, document it and turn it off when you no longer need it.

Step 5: Separate Work from Personal Browsing

Create a dedicated browser profile for work. This is one of the highest-value controls in this setup.

Use the work profile for company tools: email/workspace, source control, chat, docs, hosting, cloud, registrar access, password manager, and similar services.

Do not use that profile for personal browsing, crypto experiments, unknown dapps, airdrops, trading, wallet testing, or random extensions. Those activities should live in a separate profile or browser.

Step 6: Clean Up Extensions

Review extensions in every browser used for work.

Remove anything you do not actively need. Be especially careful with extensions that can read or change page content, inspect traffic, manage downloads, automate browser activity, or interact with wallets.

Do not install extensions from search ads, social links, chat links, or "quick fix" instructions. If you need a new extension for work, check the publisher, permissions, reviews, and installation source before installing it.

Step 7: Secure Accounts

For work-related accounts:

- Use the password manager.
- Use unique passwords.
- Prefer passkeys where supported.

- Use hardware security keys for critical accounts where possible.
- Review recovery email and phone settings.
- Remove stale sessions and unknown devices.

Critical accounts include email/workspace, source control, chat, password manager, hosting, cloud, registrar, docs, treasury tooling, and wallet-related services.

Step 8: Remove Local Secrets

Macs collect sensitive material over time. Check the obvious places first:

- Downloads
- Desktop
- Screenshots
- Notes
- Chat attachments
- Shell history
- `.env` files
- SSH private keys
- Access tokens
- API keys
- Wallet seed phrases or private keys
- Apple Passwords and Keychain entries that are no longer needed

Production secrets should not live on a work laptop unless there is a documented reason. If a secret has been shared through chat or stored locally for convenience, treat that as something to clean up, not as normal practice.

8. Extra Rules for Critical-Access Users

Some people have access where a laptop compromise could become a company-level incident. This includes production administrators, release owners, DNS or registrar admins, treasury signers, source-control organization admins, and anyone with cloud/KMS or signing authority.

If this applies to you, use the stricter profile below.

Control	Requirement
Dedicated work context	Use a dedicated work device where practical. If that is not possible, use a dedicated local user account or browser profile for privileged work.
Hardware-backed MFA	Use passkeys or hardware security keys for critical accounts where supported.
Apple Passwords / iCloud	Do not store critical credentials or synced passkeys in personal iCloud Keychain unless explicitly accepted by the team.
Password manager	Use the team-approved password manager for normal work credentials, but do not treat synced vault passkeys as hardware-bound credentials.
Browser extensions	No unapproved extensions in the production or admin browser profile.
SSH and tokens	Keep SSH keys and API tokens scoped, separate from personal use, and out of synced folders. Prefer hardware-backed SSH keys for sensitive access.
Wallet separation	Do not combine personal wallet activity with production or admin browser sessions.
Remote access	Keep SSH, screen sharing, and remote management disabled unless explicitly needed.
Travel	Do not travel with all critical devices, signing

	devices, or recovery material together.
Suspicious activity	Rotate relevant credentials and tokens before resuming privileged work.
Lockdown Mode	Consider Apple Lockdown Mode only if you are highly targeted and can tolerate the usability impact.

9. Things To Avoid

These habits are common, but they create unnecessary risk.

- Installing browser extensions casually.
- Installing wallet extensions from search results, ads, social posts, or chat links.
- Keeping company credentials in Apple Notes, screenshots, local files, chat, shell history, or personal iCloud Drive.
- Using Apple Passwords or iCloud Keychain for critical work credentials without team agreement.
- Treating synced password-manager passkeys as equivalent to hardware-bound credentials.
- Syncing private SSH keys through iCloud, Dropbox, Google Drive, or similar services.
- Using the same browser profile for personal wallet activity and production or admin work.
- Leaving Remote Login, Screen Sharing, or Remote Management enabled without a clear need.
- Running terminal commands pasted from strangers, support chats, Telegram, Discord, social media, or search results.
- Granting Accessibility, Full Disk Access, screen recording, or profile installation permissions without understanding why they are needed.
- Treating a suspicious personal wallet event as unrelated to work when the same device is used for company access.

10. If Something Suspicious Happens

For a serious suspected compromise, do not try to "clean up" first. The safer sequence is: isolate the device, preserve evidence, and use a clean device to revoke access.

Immediate Actions

1. Stop using the device for work.
2. Disconnect the device from the network: turn off Wi-Fi and unplug Ethernet.
3. Keep the device powered on and locked if you can do so safely. Do not keep working on it.
4. Do not delete files, clear logs, uninstall tools, or "clean up" before someone has decided whether evidence matters.
5. Use a different trusted device to notify the security owner or head of engineering.

Powering off is acceptable if you cannot isolate the device, if you believe it is actively causing harm, or if you are dealing with theft, seizure, or personal safety. Otherwise, leave it powered on and disconnected so there is a better chance of understanding what happened.

Revoke Access from a Clean Device

From a different trusted device, force sign-out and revoke sessions for accounts used on the suspect Mac.

Account Type	Action
Email / workspace	Sign out all sessions, review trusted devices, rotate password if needed, review OAuth apps.
Source control	Revoke sessions, remove unknown SSH keys, revoke personal access tokens, rotate affected tokens.
Password manager	Sign out other sessions, review device list, rotate exposed vault items.
Chat / docs / hosting / cloud / registrar	Revoke sessions, review connected apps, rotate credentials where available.

Cloud / KMS-related access	Revoke sessions, rotate keys, review IAM users, roles, access keys, and recent activity.
SSH	Remove affected public keys from servers and source-control accounts, then generate new keys from a clean device.
Wallets / treasury tooling	Treat as high risk. Stop signing until the device and credentials have been reviewed.

Rotate Credentials

Rotate anything that may have been exposed:

- Passwords used on the device.
- Passkeys or security keys registered from the device, if compromise is plausible.
- Personal access tokens.
- SSH keys.
- API keys.
- Cloud access keys.
- Wallet-related credentials.
- Recovery codes stored locally or in iCloud/Apple Passwords.

If the password manager was unlocked during the incident, assume more exposure and rotate the most sensitive credentials first.

Decide Whether to Rebuild

If compromise cannot be ruled out, rebuild the device before using it for work again. A rebuild should include:

- Wipe and reinstall macOS.
- Reapply this baseline.
- Reinstall only required software.
- Recreate SSH keys and tokens from a clean state.
- Reconnect accounts only after old sessions have been revoked.

If you have critical access, do not resume production, admin, treasury, DNS, or release work from the device until the security owner agrees it is safe.

11. Monthly Self-Check

Once a month, do this short review. It takes a few minutes.

Check	Done
macOS is up to date.	
FileVault is on and the recovery key is stored safely.	
Firewall is on.	
Unused sharing services are off.	
Screen lock is set to 5 minutes or less.	
The work browser profile is separate from personal browsing.	
Browser extensions have been reviewed.	
Critical accounts use hardware-backed MFA where supported.	
Normal work credentials are in the team-approved password manager.	
Apple Passwords / iCloud Keychain use has been reviewed for work credentials.	
SSH keys, access tokens, and API keys have been reviewed.	
No company secrets are sitting in obvious local or iCloud-synced locations.	
Stale sessions, devices, and tokens have been reviewed.	

12. References

- CIS Apple macOS Benchmarks: https://www.cisecurity.org/benchmark/apple_os
- NIST macOS Security Compliance Project: https://pages.nist.gov/macos_security/
- Apple Platform Security: https://support.apple.com/guide/security/welcome/web
- Apple Business Essentials: https://www.apple.com/business/essentials/
- Apple Automated Device Enrollment: https://support.apple.com/en-euro/102300
- Apple configuration profiles: https://developer.apple.com/documentation/devicemanagement/configuring-multiple-devices-using-profiles
- NIST configuration profiles: https://pages.nist.gov/macos_security/configuration-profiles/what-are-configuration-profiles/
- Microsoft Intune custom Apple settings: https://learn.microsoft.com/en-in/intune/device-configuration/templates/configure-custom-settings-apple
- Jamf Now: https://www.jamf.com/products/jamf-now/
- Apple FileVault: https://support.apple.com/guide/security/sec4c6dc1b6e/web
- Apple macOS firewall security: https://support.apple.com/guide/security/seca0e83763f/web
- Apple iCloud Keychain setup: https://support.apple.com/en-us/109016
- Apple Keychain Access on Mac: https://support.apple.com/kb/PH20093
- Apple Lockdown Mode: https://support.apple.com/en-us/105120