SETUP GUIDE

Windows Security Setup Guide for Web3 Teams

A self-service baseline that works without device management

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 Windows PC for work, whether you are a developer, an operator, or in a non-technical role. Most of the setup is designed to work **without centralized device management (MDM/Intune)**: you should be able to apply the baseline yourself, without turning your PC into a centrally managed device. Section 2 describes lightweight management options for teams that decide they want them.

The aim is not to make every PC identical. The aim is to keep a normal laptop problem, such as a bad browser extension, a suspicious download, a stolen session, or an unlocked screen, from turning into a company-wide incident.

> **NOTE**
>
> **Baseline rule:** any PC 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.

Note on editions: full BitLocker, Group Policy, and several controls below require Windows Pro, Enterprise, or Education. Windows Home offers a reduced subset (for example, "Device encryption" instead of manageable BitLocker). Where an edition matters, it is called out.

2. Lightweight Management Options for Company PCs

This guide is deliberately self-service friendly. It does not require Intune or any 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 PCs, 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
Microsoft 365 Business Premium	Small team already on Microsoft 365 that wants Entra ID, Intune, and Defender in one bundle.	Includes Intune device management and conditional access. Good low-friction starting point for company-owned Windows devices.
Microsoft Intune plus Entra ID	Team that wants automated enrollment (Windows Autopilot), policy, and conditional access.	Entra ID handles identity and enrollment; Intune is the policy and compliance control plane.
Third-party RMM/MDM (NinjaOne, ManageEngine, Workspace ONE)	Team that wants management without committing to the Microsoft stack.	Useful for inventory, patching, BitLocker key escrow, and software deployment. Verify Windows coverage before committing.

Standardization Without Full MDM

For a distributed team without Intune, you can still distribute consistent settings:

- **Provisioning packages (`.ppkg`)** built with Windows Configuration Designer. The closest analog to a macOS configuration profile: bundle Wi-Fi, certificates, restrictions, and policies into a file users apply themselves.

- **Group Policy (`gpedit.msc`)** for local policy on Pro and above, or a documented set of registry settings.
- **PowerShell baseline scripts** and the **Microsoft Security Compliance Toolkit** baselines for repeatable hardening.

Treat these as standardization, not full management. They do not replace MDM for inventory, remote wipe, BitLocker recovery-key escrow, forced updates, app deployment, or reliable offboarding.

A Sensible First Management 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:

- BitLocker on, with recovery key escrowed;
- automatic Windows Update;
- screen lock and sign-in requirement;
- Windows Defender Firewall on for all profiles;
- unused sharing and remote 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 management for company PCs where the company has a legitimate need to enforce and recover the device.

3. Quick Setup Checklist

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

Windows Settings

Setting	What To Do	Where To Check
Updates	Install pending updates. Keep automatic updates on.	Settings > Windows Update
Encryption	Turn on BitLocker (Pro and above) or Device Encryption (Home). Store the recovery key in your password manager.	Settings > Privacy & security > Device encryption, or Control Panel > BitLocker Drive Encryption
Screen lock	Require sign-in when the PC wakes. Use a short screen-saver timeout with "On resume, display logon screen."	Settings > Accounts > Sign-in options
Firewall	Turn on Microsoft Defender Firewall for Domain, Private, and Public profiles.	Windows Security > Firewall & network protection
Sharing and remote access	Turn off network discovery and file/printer sharing you do not use. Disable Remote Desktop and Remote Assistance unless needed.	Settings > Network & internet, and Settings > System > Remote Desktop

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, Vaults, and Local Data

Area	What To Do
Passwords	Store work credentials in the team-approved password manager. Do not store them in Notepad, Sticky Notes, screenshots, chat, command history, or local files.
Browser / Microsoft account sync	Edge and a personal Microsoft account can sync passwords and passkeys to your personal devices. Use them for work credentials only when the team accepts that sync model.
MFA	Prefer passkeys where supported. Use Windows Hello (TPM-bound) or FIDO2 hardware security keys for critical accounts.
Local secrets	Check Downloads, Desktop, screenshots, Sticky Notes, clipboard history, PowerShell history, WSL home directories, `.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 OneDrive, 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, but it is not equivalent to 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.
Edge / Microsoft account sync, Windows Credential Manager	Personal credentials, and low-risk work credentials if the team accepts the sync model.	Credentials and passkeys may sync to personal devices outside company visibility. Credential Manager secrets are protected by DPAPI and unlock with your sign-in.
Windows Hello (TPM-bound passkey)	Strong, hardware-backed sign-in on a specific device.	Bound to that device and not portable; enroll a backup method.
FIDO2 hardware security key	Critical accounts such as email/workspace, source-control admin, cloud, hosting, registrar, and password-manager admin.	Less convenient, but portable and bound to a physical authenticator.
Hardware-backed SSH key (FIDO2 `sk-ed25519`)	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 Windows Hello or FIDO2 hardware keys 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 browser sync, Credential Manager, Sticky Notes, screenshots, or local files.
- If browser or Microsoft account sync holds a work credential, understand that every synced device becomes part of the access surface.

5. Browser Sync, Microsoft Account, and OneDrive

Edge sync, a personal Microsoft account, and OneDrive are convenient and well-designed for personal use. The problem in a work context is that they can sync work credentials, passkeys, and files into personal devices that the company does not know about and cannot clean up during offboarding or an incident.

Recommended Approach

Topic	Guidance
Edge password sync	Use it for personal credentials. For work credentials, use the team-approved password manager by default.
Microsoft account sync	Treat sync as a path to every device signed in to the same personal Microsoft account. If a work credential or passkey is stored there, every synced device becomes part of the access surface. Prefer a separate work account context.
Passkeys	Passkeys are good, but synced passkeys are still credentials. For critical accounts, prefer Windows Hello or FIDO2 hardware keys.
Windows Credential Manager	It is normal for apps and the OS to store some tokens there. Do not manually store production secrets, seed phrases, API keys, KMS material, recovery keys, or SSH private keys there for convenience.
OneDrive	Do not keep work secrets or confidential files in personal OneDrive, including OneDrive-backed Desktop and Documents folders. Use the approved company storage location.

If you use browser or Microsoft account sync for any work credential, make sure:

- Your Microsoft account has a strong unique password and MFA.

- No one else uses your Microsoft account.
- Every synced device is encrypted, updated, and locked.
- Old or unused devices have been removed from the account.
- You understand that incident cleanup may require reviewing every synced device, not only the PC 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. On Windows, keys live in `%USERPROFILE%\.ssh`.
- Prefer modern key types such as ed25519 unless a service requires something else.
- Protect file-based private keys with a passphrase. Set the OpenSSH `ssh-agent` service to start automatically rather than leaving keys unprotected.
- For production or sensitive infrastructure access, prefer hardware-backed SSH keys (FIDO2 `sk-ed25519`).
- Do not store private keys in OneDrive, 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.
- If you use WSL, remember it has its own home directory and shell history. Treat keys and secrets inside WSL with the same care.

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 Windows

Open **Settings > Windows Update**. Install anything pending and keep automatic updates on.

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 BitLocker

Open **Control Panel > BitLocker Drive Encryption** (Pro and above) or **Settings > Privacy & security > Device encryption** (Home) and enable encryption for the system drive.

Save the recovery key in your password manager. Do not rely only on saving it to a personal Microsoft account, and do not save it as a screenshot, local file, or chat message on the same PC. A recovery key stored on the device it unlocks does not protect that device. If your device does not support encryption, raise it with the team rather than skipping it silently.

Step 3: Lock the Device Properly

Open **Settings > Accounts > Sign-in options**.

- Set "When PC wakes up from sleep" to require sign-in.
- Set a short screen-saver timeout with "On resume, display logon screen" enabled.
- Lock the screen manually with **Win+L** 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 **Windows Security > Firewall & network protection** and confirm the firewall is on for Domain, Private, and Public profiles.

Then turn off what you do not actively use:

- Remote Desktop (Settings > System > Remote Desktop)

- Remote Assistance (System Properties > Remote)
- Network discovery and file/printer sharing on public networks
- Nearby sharing
- "Project to this PC"

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 baseline.

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 Windows Hello or FIDO2 hardware keys for critical accounts.
- 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

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

- Downloads
- Desktop
- Screenshots (Pictures\Screenshots)
- Sticky Notes
- Clipboard history (Win+V)
- PowerShell history (`%APPDATA%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt`)
- WSL home directory and shell history, if you use WSL
- `.env` files
- SSH private keys (`%USERPROFILE%\.ssh`)
- Access tokens
- API keys
- Wallet seed phrases or private keys
- Windows Credential Manager 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 Windows Hello for Business or FIDO2 hardware keys for critical accounts where supported.
Sync hygiene	Do not store critical credentials or synced passkeys in a personal Microsoft account or Edge sync 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 Remote Desktop and Remote Assistance 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.
Attack-surface reduction	Consider Smart App Control or S Mode, enable Core Isolation (memory integrity), and keep installed software minimal. Windows has no single ”lockdown” toggle; reduce surface deliberately.

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 Notepad, Sticky Notes, screenshots, local files, chat, command history, or personal OneDrive.
- Using browser or Microsoft account sync for critical work credentials without team agreement.
- Treating synced password-manager passkeys as equivalent to hardware-bound credentials.
- Syncing private SSH keys through OneDrive, Dropbox, Google Drive, or similar services.
- Using the same browser profile for personal wallet activity and production or admin work.
- Leaving Remote Desktop, Remote Assistance, or file sharing enabled without a clear need.
- Running PowerShell or Command Prompt commands pasted from strangers, support chats, Telegram, Discord, social media, or search results. Be especially wary of `mshta`, `curl | iex`, and "press Win+R and paste this" instructions.
- Approving UAC prompts, disabling Defender, or installing software without understanding why.
- 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 PC.

Account Type	Action
Microsoft 365 / Entra ID	Sign out all sessions, review registered devices, rotate password if needed, review OAuth and enterprise app consents.
Email / workspace	Sign out all sessions, review trusted devices, rotate password if needed, review connected 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 browser/account sync.

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 Windows (a clean reinstall, not just "Reset this PC" with apps kept).
- 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 should take a few minutes.

Check	Done
Windows is up to date.	
BitLocker or Device Encryption is on and the recovery key is stored safely.	
Defender Firewall is on for all profiles.	
Remote Desktop and unused sharing are off.	
Sign-in is required on wake and the screen-saver timeout is short.	
The work browser profile is separate from personal browsing.	
Browser extensions have been reviewed.	
Critical accounts use Windows Hello or FIDO2 keys where supported.	
Normal work credentials are in the team-approved password manager.	
Browser / Microsoft account sync 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 OneDrive-synced locations.	
Stale sessions, devices, and tokens have been reviewed.	

12. References

- CIS Microsoft Windows Benchmarks: https://www.cisecurity.org/benchmark/microsoft_windows_desktop
- Microsoft Security Baselines and Security Compliance Toolkit: https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines
- BitLocker: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/
- Windows Hello for Business: https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/
- Microsoft Defender Firewall: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/
- Microsoft Intune: https://learn.microsoft.com/en-us/mem/intune/
- Windows Autopilot: https://learn.microsoft.com/en-us/autopilot/
- Provisioning packages (Windows Configuration Designer): https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages
- Smart App Control: https://support.microsoft.com/en-us/topic/285ea03d-fa88-4d56-882e-6698afdb7003
- OpenSSH for Windows: https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_overview