WORKTIME®

REMOTE-WORK PRIVACY CHECKLIST FOR MANAGERS

1 Meeting & communication rules

□ Require employees to disable message previews
□ Require DND during all video meetings
□ Require closing personal apps/tabs before sharing screen
□ Require window-only sharing (not full screen)
□ Require microphone mute inside the meeting app, not via OS

2 Tool usage policy

□ Ban Discord, Mumble, TeamSpeak, Steam Chat (unsafe, auto-mic activation)
□ Approve only business tools for video, audio, and messaging
□ Prohibit screenshot-based monitoring tools
□ Allow only non-invasive monitoring (WorkTime – no screenshots, no keystrokes, no cameras)

3 AI & shared workspace rules

□ No shared accounts
□ No sensitive data in AI tools unless fully private workspace
□ Require checking workspace permissions before using AI tools
□ Train employees on how prompts can leak into shared company folders
□ Provide examples of real-life incidents (optional section in training)

4 Privacy-risk training topics

□ Pop-up notifications leaking private messages
□ Auto-join / auto-accept calls broadcasting unintended audio
□ OS mute confusion (speaker mute ≠ mic mute)
□ Wrong-screen sharing
□ Cameras activating early
□ Shared cloud folders exposing confidential files
□ AI prompts visible to the entire company
□ Hidden data collectors (IoT, cloud sync, extensions, old VPNs)

5 Monitoring policy

□ Communicate explicitly: “We do not use screenshots, keystrokes, webcams, or any invasive features.”
□ Communicate what metrics WorkTime collects (productivity only)
□ Emphasize trust-building and privacy-first monitoring