DOWNLOADABLE WORKSHEET · ENDPOINT MANAGEMENT

Remote Work Security *Self-Assessment*

A scored assessment of your remote and hybrid work security posture across the five areas where 2020-era setups fail — identity, device, network, data, and people — plus the AI-era threats that target remote workers specifically.

How to use this worksheet

This is an assessment of your environment as it actually operates today — not as the policy binder describes it. Most hybrid companies are still running on decisions made during the 2020 remote-work scramble; this worksheet locates exactly where those decisions are now exposing you.

Run it with evidence, not memory. For each statement, answer based on what you can verify — sign-in logs, device inventories, actual tickets — not what you believe to be configured. If you can't verify it, that's a "No."

Score every statement using the key below. Where a statement covers a population ("all devices," "every system"), score against the entire population including BYOD and contractor equipment — the unmanaged edge is the point of this exercise.

It takes about 30 minutes. If a question requires pulling a report you've never pulled before, note that too — the questions you can't answer quickly are findings in themselves.

Scoring key

Score	Answer	What it means
2	Yes	True today, verifiable with evidence, covers the full population it describes.
1	Partial	True for some systems, some users, or some device types — but you know there are gaps.
0	No	Not in place, not verifiable, or you don't know. "We think so" scores 0.

Answer honestly. A flattering score protects nothing.

©2026 Plow Networks, Proprietary & Confidential.

Area 1 — Identity (6 items · max 12 points)

Is the person asking for access actually who they claim to be — every time, on every system?

#	Statement	Score (0-2)
1.1	MFA is enforced on every system a remote user can reach from the internet — including email, the VPN or remote-access gateway itself, payroll/HR, finance, and admin portals.	☐
1.2	Legacy authentication protocols that bypass MFA (IMAP, POP, SMTP basic auth, older clients) are blocked, not just discouraged.	☐
1.3	Conditional access policies restrict sensitive applications based on device health or compliance, not just correct credentials.	☐
1.4	Sign-ins from impossible or unexpected locations are automatically blocked or challenged, and someone reviews the alerts.	☐
1.5	Privileged/admin accounts have stronger controls than standard users (separate accounts, phishing-resistant MFA, no day-to-day use).	☐
1.6	When an employee leaves, all remote access — cloud apps, VPN, cached sessions, tokens — is revoked the same day, and the process is verified rather than assumed.	☐

Area 1 total _____ / 12

©2026 Plow Networks, Proprietary & Confidential.

Area 2 — Device (7 items · max 14 points)

Do you know what devices touch company data, and can you vouch for their condition?

#	Statement	Score (0-2)
2.1	You can produce a list of every device that accessed company data in the last 30 days — and reconcile it against your managed inventory.	☐
2.2	Personal/BYOD devices are governed by a deliberate policy (what they may access, through what controls), not an inherited reality nobody chose.	☐
2.3	Patch status is visible for remote devices even when they stay off the corporate network for weeks.	☐
2.4	Disk encryption is enforced and verified on every laptop that leaves an office — not assumed from a baseline image.	☐
2.5	Endpoint detection and response (EDR) covers remote devices, and alerts from them reach the same response process as office machines.	☐
2.6	You can remotely lock or wipe company data from a lost or stolen device, including BYOD, and you have actually tested it.	☐
2.7	Contractor and third-party devices that touch your data meet defined requirements, or are restricted to controlled access paths.	☐

Area 2 total _____ / 14

©2026 Plow Networks, Proprietary & Confidential.

Area 3 — Network (6 items · max 12 points)

What did you decide to inspect, where — and what did you consciously accept that you can't?

#	Statement	Score (0-2)
3.1	Your split-tunnel vs. full-tunnel configuration is a documented decision with known visibility tradeoffs — not whatever was configured in 2020.	☐
3.2	Remote access grants reach to specific applications, not broad network-level access to a flat internal network.	☐
3.3	A single phished VPN credential would NOT give an attacker lateral reach to servers and systems beyond that user's role.	☐
3.4	Employees have written guidance for home network hygiene (router firmware, changed default passwords, separate Wi-Fi for work where practical).	☐
3.5	Security policy is enforced for remote users even when their traffic never touches the office (cloud-delivered filtering/inspection, or an explicit accepted-risk decision).	☐
3.6	Remote access capacity and performance are good enough that users don't route around the controls to get work done.	☐

Area 3 total _____ / 12

Area 4 — Data (5 items · max 10 points)

Where do company files actually end up once they leave sanctioned systems?

#	Statement	Score (0-2)
4.1	Company data is blocked or controlled from syncing to personal cloud storage accounts on devices that access company systems.	☐
4.2	Downloads to unmanaged/BYOD devices are restricted (e.g., browser-only sessions, no local file storage) for sensitive applications.	☐
4.3	You have visibility into sensitive data leaving sanctioned locations — alerts, DLP, or auditable logs someone actually reviews.	☐
4.4	Offboarding includes recovering or destroying company data on personal devices, not just disabling accounts.	☐
4.5	You have traced, within the last year, where files actually live on a sample of remote employees' machines — and acted on what you found.	☐

Area 4 total _____ / 10

©2026 Plow Networks, Proprietary & Confidential.

Area 5 — People (5 items · max 10 points)

When something feels wrong, does a defined procedure kick in — or just individual judgment?

#	Statement	Score (0-2)
5.1	There is a written, trained procedure for verifying unusual requests (payments, banking changes, credential resets) — not reliance on employees "being careful."	☐
5.2	Employees know they are safe to delay an "urgent" request from an executive while they verify it, and leadership has said so explicitly.	☐
5.3	Security awareness training has been updated within the last 12 months to reflect current attack techniques, and remote workers complete it.	☐
5.4	Remote employees have a fast, known channel to report something suspicious — and reports get acknowledged, so people keep reporting.	☐
5.5	Your remote work policy has been reviewed and reissued since it was first written — it is not a forwarded email from March 2020.	☐

Area 5 total _____ / 10

Area 6 — AI-Era Threats (5 items · max 10 points)

AI didn't invent these attacks — it industrialized the ones that work best on remote workers.

#	Statement	Score (0-2)
6.1	Your phishing defense does not depend on employees spotting typos or awkward phrasing — you assume fluent, personalized, AI-written lures and defend in layers.	☐
6.2	Any request to move money or change banking details requires a verification callback on a number from the company directory — never a number or link from the message itself.	☐
6.3	Finance and executives share a code word (or equivalent out-of-band check) for payment requests that no cloned voice or deepfake would know.	☐
6.4	An AI usage policy defines what company data may go into which AI tools — and it explicitly covers personal devices, not just managed ones.	☐
6.5	Employees have a sanctioned AI option for legitimate work, so shadow AI on unmanaged devices isn't the only path to productivity.	☐

Area 6 total _____ / 10

©2026 Plow Networks, Proprietary & Confidential.

Your score

Transfer each area total, then compute the overall percentage.

Area	Your total	Max
1 — Identity	☐	12
2 — Device	☐	14
3 — Network	☐	12
4 — Data	☐	10
5 — People	☐	10
6 — AI-Era Threats	☐	10
Overall	☐	68

Overall percentage = (your total ÷ 68) × 100

Write your percentage in the box — you'll use it to find your maturity band below.

Maturity bands

Overall score	Band	Verdict
0 - 27 points (0-40%)	Running on 2020	Your remote work security is still the emergency setup, and the emergency ended years ago. The gap between "it works" and "it's secure" is wide open — an unmanaged device with cached credentials is functionally an unlocked office. Start with the two cheapest, highest-leverage fixes: MFA on every internet-reachable system (including the VPN itself), and a written verification-callback procedure for payment requests. Do those this month; build the device inventory next.
28 - 51 points (41-75%)	Partial coverage, real gaps	You've modernized parts of the stack, but your posture is only as strong as your weakest area — and your section tallies just told you which one that is. Typical pattern in this band: strong identity on Microsoft 365, weak everywhere the managed fleet ends (BYOD, data sprawl, no AI-era procedures). Take your lowest-scoring area and close its 0-scores before adding anything new anywhere else.
52 - 68 points (76-100%)	Deliberate architecture	Your remote work security reflects decisions made on purpose, with evidence behind them. The work now is keeping it true: re-verify the populations behind your "Yes" answers quarterly (fleets drift, exceptions accumulate), rehearse the people-layer procedures before an attacker tests them for you, and re-run this assessment when anything material changes — new tools, acquisitions, or the next wave of AI-driven techniques.

©2026 Plow Networks, Proprietary & Confidential.

Reality check: Score against the whole population every statement describes. Most teams in the middle band got there by scoring their managed laptops and forgetting the personal desktop that "just checks email." If more than a third of your answers were Partial, your effective posture is one band lower than your number — Partial is where incidents actually start.

Reading your section tallies

The overall band tells you how exposed you are. The section tallies tell you where to start:

- Lowest area = first project. Remote work security fails at the weakest area, not the average.
- Identity or Device lowest → foundational gap; fix before anything else, because every other control assumes these.
- Network lowest → you're still betting everything on the tunnel; revisit what you inspect, where, and what access a single credential grants.
- Data or People lowest → your technical stack is ahead of your operational discipline; these are policy-and-procedure fixes that cost far less than tooling.
- AI-Era Threats lowest → your controls were designed for attacks that have since been industrialized; the countermeasures (callbacks, code words, AI usage policy) are cheap and fast to deploy.

Lowest-scoring area:

First action:

Re-assessment date (quarterly recommended):

Remember: A remote work setup that "works" and one that's secure are different claims. This worksheet measures the second one.

Not Sure What Your Remote Setup Is Actually Exposing?

Plow helps hybrid teams replace 2020-era emergency setups with deliberate remote work security — identity, devices, network, data, and the AI-era threats that target them.

Request a Remote Work Security Assessment →