Small Time Devs - New client onboarding

This tells us what you run and what you need, so your first call is about decisions, not questions. Only 7 questions are required to start (marked *); the rest helps us prepare. Skip anything you don't know - we will find it together.

How to send this back to us

1. Fill it in: type your answers in the Word file, or print the PDF and write on it.
2. Save it. If you wrote on paper, scan it or take a clear photo of every page.
3. Email it to **support@smalltimedevs.com** with the subject: Onboarding - your company name.
4. We reply by email to book a short intro call. Then, with the access you approve, we connect remotely for a free look-only check and send you our findings and an exact written quote.

Never put passwords, PINs, API keys, tokens, recovery codes, BitLocker keys, MFA codes, VPN keys or secret answers in this form or this document. Accounts you create for us are handed over only by a one-time secure share or live on a call.

1. Company and contacts informed by NIST CSF GV.OC

Legal company name *

Who referred you? (name or referral code - optional)

Industry

How many people use computers or email? *

Office locations (city, state) and how many people at each

Main contact (name, role, email, phone) *

After-hours / emergency contact

Who can approve work and sign agreements?

Billing contact (name, email)

2. What you want from us

Services

☐ Managed Microsoft 365 & security ☐ Security audit ☐ AI automation ☐ Full IT support

☐ Not sure yet

Top 3 problems you want solved *

Any deadline (renewal, audit, launch)?

3. Written authorization and scope informed by Legal cover for scans and audits

☐ You authorize Small Time Devs to connect remotely, with the access you approve, and to scan and review the domains, Microsoft 365 tenant and devices listed in this form. During the free check we look only and change nothing. *

Your full name and title (as authorizing signer) *

Anything we must NOT touch or scan

4. Microsoft 365 / email informed by CIS 1, 2, 5; NIST CSF ID.AM

Email and files platform

☐ Microsoft 365 ☐ Google Workspace ☐ Other ☐ None yet

Your domains (e.g. example.com) *

Licenses you have today (e.g. Business Basic, Premium) and how many

Where your domains are registered / who runs DNS

Shared mailboxes, distribution lists, or service accounts you know of

5. Admin access we will need informed by CIS 5, 6; Microsoft GDAP; emergency access accounts

We will send you a Microsoft partner (GDAP) request to approve, ask for a named admin account for our engineer with MFA, and ask for a DNS user at your registrar. You keep two emergency (break-glass) accounts that only you control.

Will you approve a Microsoft partner (GDAP) access request from Small Time Devs?

☐ Yes ☐ Need to discuss ☐ No

Who are your current global admins (names only)?

Do you have emergency (break-glass) admin accounts?

☐ Yes, tested recently ☐ Yes, never tested ☐ No ☐ Don't know

Is two-step sign-in (MFA) on for everyone?

☐ Everyone ☐ Some people ☐ No one ☐ Don't know

Do you use a password manager? Which?

6. Remote access and service accounts informed by CIS 5, 6, 12

To manage your systems we usually need accounts created for us and a secure way in. You create the accounts; we send you the exact list after this form. Credentials are handed over only through a one-time, expiring secure share (for example a password-manager share link) or set up live on a call - never in this form, by email or by text. Remote desktop (RDP) is never opened directly to the internet: it goes through a VPN, a remote-desktop gateway or a zero-trust tunnel, with MFA, and limited to our addresses where possible.

Accounts we will need (tick what applies)

☐ Named admin for our engineer (Microsoft 365 / Entra)

☐ Domain / server admin (on-premises Active Directory) ☐ Firewall / router admin ☐ Backup console

☐ Line-of-business app admin ☐ Service account for monitoring or backup jobs

☐ DNS / registrar user ☐ Not sure

Servers or PCs we must reach remotely (names or roles, OS, on-site or cloud)

How do people or vendors connect remotely today?

☐ VPN ☐ Remote Desktop Gateway ☐ RDP open to the internet

☐ Remote-support tool (TeamViewer, AnyDesk, ScreenConnect...) ☐ Zero-trust tunnel ☐ None

☐ Don't know

Which way in may we use?

☐ Your VPN ☐ A remote-desktop gateway ☐ A remote-support tool you approve

☐ A zero-trust tunnel we set up with you ☐ Let's decide on the call

Can your firewall limit access to our IP addresses (we send them)?

☐ Yes ☐ No ☐ Don't know

When may we connect (business hours only, any time, by request)?

Who approves new access and is told when we connect?

How should account details reach us?

☐ One-time secure share link (password manager) ☐ Set up live on a call

☐ Your preferred secure method (tell us)

7. Devices informed by CIS 1, 4, 7, 10

How many laptops/desktops, phones, tablets, servers?

Operating systems (Windows 11, macOS, ...)

Current antivirus / endpoint protection

Are devices managed (Intune or similar)?

☐ Yes ☐ Some ☐ No ☐ Don't know

How do updates get installed today?

Do people use personal devices for work?

☐ Yes ☐ No ☐ Some

8. Email and web protection informed by CIS 9

Has anyone sent fake email pretending to be you?

☐ Yes ☐ No ☐ Don't know

Spam / phishing filtering in use

9. Data and backup informed by CIS 3, 11

Where does important data live (OneDrive, SharePoint, file server, apps)?

Regulated data you handle

☐ Health (HIPAA) ☐ Card payments (PCI) ☐ Defense / CUI (CMMC) ☐ Personal data of customers

☐ None ☐ Not sure

Is Microsoft 365 backed up today? By what?

If you lost data, how much (hours/days) could you afford to lose?

How long could you be down before it hurts badly?

Your most critical systems or apps

10. Network informed by CIS 12

Internet provider and firewall / router brand

How do people work remotely (VPN, cloud only, ...)?

Guest Wi-Fi separate from staff Wi-Fi?

☐ Yes ☐ No ☐ Don't know

11. People and process informed by CIS 5, 14

How do new hires get accounts, and how are leavers removed?

Any security / phishing training?

☐ Yes, regular ☐ Once ☐ No

12. Vendors and apps informed by CIS 15; NIST CSF GV.SC

Current or past IT providers

Main software and online services you rely on

13. Incidents and insurance informed by CIS 17

Any past breaches, hacks, ransomware or lost devices?

Do you have cyber insurance? Any requirements from it?

14. AI automation (optional)

Repetitive tasks you'd like off your plate

Data an assistant may NOT see

How to send this back to us

1. Fill it in: type your answers in the Word file, or print the PDF and write on it.
2. Save it. If you wrote on paper, scan it or take a clear photo of every page.
3. Email it to **support@smalltimedevs.com** with the subject: Onboarding - your company name.
4. We reply by email to book a short intro call. Then, with the access you approve, we connect remotely for a free look-only check and send you our findings and an exact written quote.

* required. Informed by: CIS Critical Security Controls v8.1, Implementation Group 1 (https://www.cisecurity.org/controls/v8-1); NIST Cybersecurity Framework 2.0 (CSWP 29) (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf); Microsoft: granular delegated admin privileges (GDAP) (https://learn.microsoft.com/en-us/partner-center/customers/gdap-introduction); Microsoft: emergency access accounts (https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access). Small Time Devs Inc, Wyoming. Version 2026-11-12 draft 2.