



Cloud Control Checklist

*Lock your side of the door — Microsoft 365, Google Workspace, devices and remote work. Get your calendar open; this is about an hour. It's likely you'll need IT support to help with this. See Chapter 4 of *Shit, I've Been Hacked!* for more detail.*

1. Confirm MFA is enabled on every cloud platform — email, accounting, CRM, file storage.
2. Identify who has admin access in each system. If you're unsure, ask your IT provider.
3. Separate your daily-use account from any admin accounts.
4. Confirm full-disk encryption is enabled on every business device.
5. Get rid of any shared logins.
6. Review email forwarding settings and inbox rules in all accounts — especially finance.
7. Check when a staff member last left. Was their access removed the same day?
8. Turn on Conditional / Context-aware Access if your plan offers it.
9. Do a website TLS check to confirm your public site is served over HTTPS.

One question to answer honestly: if someone logged into our primary cloud account at midnight tonight, would we know by morning? If not — that's the gap to close.