INNOVA
GROUP

Technology That Works. Innovation That Lasts.

HOW-TO GUIDE

Working From Anywhere, Securely

How to let people work from home, a client site or a hotel without quietly giving away control of your business.

Identity · Devices · Data · People

Innova Technologies Group Ltd · Hull, United Kingdom
v1.0 · July 2026
innovagroup.tech

BEFORE YOU START

Remote working happened. Securing it mostly didn't.

Most businesses enabled working from anywhere quickly, out of necessity, and never went back to do it properly. The arrangements put in place for a few weeks are, years later, simply how the business runs.

That matters because the old model of security no longer applies. It assumed the important things sat in the office, behind the office firewall, on machines in the building. Now the files are in the cloud, the laptops are in kitchens and hotel rooms, and the office firewall protects an increasingly empty room.

This guide covers what actually protects a business whose people work anywhere. It is deliberately practical, and most of it uses licensing you already own rather than anything new.

Who it is for. Owners and managers of businesses where at least some people work outside the office some of the time. No technical background assumed.

A note on friction. Security that makes work difficult gets bypassed — people use personal email, personal cloud storage, their own phone. Everything recommended here is chosen to be close to invisible once in place. If a control is annoying people daily, it is the wrong control.

> TWO THINGS TO NOTE
>
> This guide refers to Microsoft 365 capabilities throughout, and availability varies by plan — the more advanced device and access controls sit in higher tiers such as Business Premium. It also overlaps deliberately with our security and IT guides, because remote working is where identity, devices and data meet.

WHAT THIS GUIDE COVERS

INNOVA GROUP

THE PRINCIPLE

The office walls stopped mattering

What matters now is who is signing in, from what device, to reach which data.

For years, being inside the building was treated as proof of trustworthiness. Anything on the office network was assumed to be fine; anything outside it was not. That assumption is now almost meaningless: the systems people use are reached over the internet from wherever they happen to be, and the office network is simply one more place they connect from.

Replacing it is a simple idea. Trust is established each time someone signs in, based on four things you can actually control.

01 **Who they are**
Proven properly, with more than a password. This is the control that does most of the work, and the one to get right first.

02 **What they are using**
A managed, encrypted, up-to-date device rather than an unknown machine in a hotel business centre.

03 **What they are reaching**
Payroll deserves stricter conditions than the staff handbook. Not everything needs the same protection.

04 **Whether anything looks wrong**
A sign-in from a country you do not operate in, at three in the morning, on an unrecognised device. Worth blocking automatically.

> THE REASSURING PART
>
> None of this requires new infrastructure. In a Microsoft environment it is configuration — identity, device policy and access rules — using capability most businesses already pay for and have never switched on.

SECTION ONE

Identity Is The New Perimeter

If you do one thing from this guide, do this section. Nearly every remote-working compromise starts with a stolen password.

- [ ] **Multi-factor authentication on every account**
  No exceptions, including directors and anyone who has asked to be excluded. Away from the office, this is what stands between a leaked password and a compromised business.
- [ ] **Use an authenticator app, not text messages**
  Quicker for staff and considerably harder to intercept. Passkeys are stronger still where your plan and devices support them.
- [ ] **Block sign-ins from places you do not operate**
  If nobody works outside the UK and Ireland, sign-ins from elsewhere can be refused automatically. Simple, effective, and invisible to staff.
- [ ] **Require a managed device for sensitive systems**
  Finance, HR and admin functions reachable only from company-managed devices — not from a personal laptop or an internet café.
- [ ] **Keep administrator accounts separate**
  Nobody should read email from an account that can reconfigure your tenancy, least of all over hotel wi-fi.
- [ ] **Remove leavers the same day**
  Remote access outlives a desk. An account that still works from anywhere is a far larger exposure than one needing a building.
- [ ] **Know how to lock someone out quickly**
  A lost laptop or a suspected compromise needs sessions revoked in minutes. Make sure someone knows how, before it is needed.

> WHERE MICROSOFT HELPS
>
> All of the above is delivered through **Entra ID** and **Conditional Access** — rules about who can sign in, from where, on what, and to reach which data. **Availability depends on your Microsoft 365 licence**, with the more advanced rules in higher tiers.

SECTION TWO

Devices You Can Trust

A laptop at home is not protected by anything in your office. Whatever protects it has to travel with it.

- [ ] **Encrypt every device**
  BitLocker on Windows, FileVault on Mac. Without it, a laptop left on a train is a data breach; with it, an insurance claim.
- [ ] **Enforce a screen lock**
  A PIN, password or biometric, locking automatically after a short period. Kitchen tables, cafes and client sites all have passers-by.
- [ ] **Keep updates automatic**
  Operating system and applications, without relying on individuals to accept prompts. Remote machines drift out of date fastest.
- [ ] **Endpoint protection on everything**
  Active, current, and with alerts somebody actually reads. Protection nobody monitors is not protection.
- [ ] **Enable the device firewall**
  The one built into Windows and macOS, enforced centrally, since there is no office firewall on hotel wi-fi.
- [ ] **Be able to wipe a device remotely**
  For loss or theft. On personal devices, wiping just the work data is usually the right and more acceptable option.
- [ ] **Decide about personal devices deliberately**
  Most businesses allow work email on personal phones. That is fine — as a decision, with basic conditions attached, rather than something that simply happened.

> WHERE MICROSOFT HELPS
>
> **Intune** applies all of this to every device wherever it is, and reports which are compliant. Combined with Conditional Access, a device that falls out of compliance can lose access until it is fixed. **Availability depends on your Microsoft 365 licence.**

SECTION THREE

Home & Public Networks

Less dangerous than people assume, but worth a few sensible rules — and worth being honest about what a VPN does and does not do.

Almost everything staff use is now reached over an encrypted connection, so a café network cannot simply read their email. The realistic risks are more mundane: someone reading a screen over a shoulder, a device left unattended, a fake wi-fi network, or a connection so poor that people give up and use something unapproved instead.

SituationWhat actually matters Home wi-fiRouter admin password changed from the default, firmware kept updated, and a decent wi-fi password. That is genuinely enough for most people. Public wi-fiFine for normal work on a managed device. Avoid networks with no password, and be wary of lookalike names. A mobile hotspot is usually better. Client sitesTreat as public. Never let a client's IT connect to your machine, and do not plug in unknown drives or cables. Hotels and airportsWhere shoulder-surfing genuinely happens. A privacy screen costs little if someone travels regularly. Shared or family computersShould not be used for work at all. There is no way to know what else is on them.

ON VPNS, HONESTLY

A VPN is needed to reach something still sitting inside your office — an old server or line-of-business system. It is not a general security measure, and for cloud services it adds little beyond another thing to break. If you use one only because it was always there, that is worth reviewing.

> **THE FRICTION POINT WORTH WATCHING**
>
> If connecting is slow or awkward, people work around it — personal email, personal cloud storage, files on the desktop. Poor remote access does not just frustrate staff; it actively creates the shadow systems you least want.

SECTION FOUR

Where The Data Lives

Remote working goes wrong most often not through an attack, but through work quietly ending up somewhere nobody can see.

- [ ] **Everything in SharePoint, Teams or OneDrive**
  Not the desktop, not a USB stick, not personal cloud storage. If it is not in your environment, it is not backed up, searchable or recoverable.
- [ ] **Back up Desktop and Documents automatically**
  OneDrive can protect these folders without anyone thinking about it — which quietly prevents most remote data loss.
- [ ] **Share links, never attachments**
  Especially remotely, where emailed copies multiply fastest. One file, one version, access you can withdraw later.
- [ ] **Ban personal email and personal cloud storage for work**
  The most common and least visible leak. Usually a symptom of official tools being awkward — so fix that too.
- [ ] **Review external sharing occasionally**
  Links created for a client two years ago often still work. Twice a year is enough to keep this tidy.
- [ ] **Set clear rules for AI tools**
  Which are approved, and what company or client data may go into them. Copilot inside your tenancy is a very different proposition to a public chatbot.
- [ ] **Remember cloud is not backup**
  Microsoft 365 protects against its own failures, not against deletion, corruption or ransomware inside your tenancy.

> THE PRINTING QUESTION
>
> People print at home, and home printing means company documents in domestic bins and on kitchen worktops. Worth a sentence in your policy about what should not be printed, and how to dispose of what is.

SECTION FIVE

People & Habits

Working alone changes behaviour. The colleague you would have turned to is no longer sitting opposite, and attackers know it.

In an office, someone asked to change a supplier's bank details would probably mention it out loud, and somebody would query it. Remotely, that conversation does not happen — which is precisely why invoice fraud and impersonation work so much better against distributed teams.

- [ ] **Verify money and bank changes by phone, always**
  On a number you already had. This single habit prevents the most expensive fraud affecting UK businesses, and remote working removes the informal checks that used to catch it.
- [ ] **Make reporting easy and blameless**
  One obvious route, and thanks rather than blame. Remote staff hesitate longer before admitting a mistake, and hesitation is what causes the damage.
- [ ] **Expect impersonation of senior people**
  "I'm in meetings all day, just email me back" is the standard opening. Agree that verifying by phone is always acceptable, never rude.
- [ ] **Give new starters a real induction**
  A remote starter can go weeks without meeting anyone. Make sure they know who to ask, and what the business does and does not do.
- [ ] **Watch for security theatre**
  If a control is bypassed daily, it is not working. Ask why rather than restating the rule.
- [ ] **Keep the handouts where people see them**
  Phishing, passwords and sign-in prompts. Short reminders repeated occasionally beat annual training nobody remembers.

> **A CULTURAL POINT WORTH MAKING**
>
> The businesses that handle this best are not the ones with the strictest rules. They are the ones where saying "this looks odd, can you check?" is completely normal — from anyone, to anyone, at any level.

SECTION SIX

What Goes Wrong

Eight patterns we see repeatedly in businesses that enabled remote working quickly and never revisited it.

- [ ] **Emergency arrangements that became permanent**
  Personal laptops, a hastily opened remote connection, shared logins “just for now”. Years later it is simply how things work.
- [ ] **MFA on some accounts but not all**
  Usually the senior people who found it irritating — who are also the most impersonated and have the most access.
- [ ] **Personal devices doing real work, unmanaged**
  Not inherently wrong. Unknown and unconditional is the problem.
- [ ] **Work saved locally because sync is awkward**
  Unbacked-up, invisible, and lost when the laptop fails. Almost always a symptom of poor setup rather than carelessness.
- [ ] **A VPN kept out of habit**
  Slow, fragile, and no longer protecting anything, because everything it fronted now lives in the cloud.
- [ ] **Leavers who keep working remotely**
  Nobody collected a laptop, nobody disabled the account. With remote access, neither is required to keep using it.
- [ ] **No way to reach anyone when it breaks**
  A remote worker with a dead laptop and no route to support simply stops working for the day.
- [ ] **A policy nobody has read**
  Written in 2020, filed, never mentioned again. A page people remember beats twelve pages they have not seen.

SECTION SEVEN

Where To Start

In order. The first three matter far more than the rest, and none of them is a project.

01 **Multi-factor authentication on every account**
Including the exceptions. Days rather than weeks, usually with licensing you already hold.

02 **Confirm every device is encrypted and updating**
Including the ones that rarely come into the office. Establish the facts rather than assuming.

03 **Get local work into OneDrive and SharePoint**
Then fix whatever made people save locally in the first place, or it will happen again.

04 **Agree the phone-verification rule for money**
One sentence, said out loud to everyone. Costs nothing and prevents the most expensive incident.

05 **Write one page people will actually read**
Where files go, which tools are approved, how to report a problem, and who to call. One page, kept current.

> WHAT GOOD LOOKS LIKE
>
> People work the same way wherever they are, nothing important lives only on a laptop, a lost device is an inconvenience rather than an incident, and somebody can revoke access within minutes of being asked.

INNOVA
GROUP

NEXT STEPS

Most of this is already paid for.

Nearly everything in this guide is configuration of a Microsoft environment you already own, rather than new products. That is the honest reason to start with what you have before buying anything.

If you would like a second opinion on how your remote setup stands, or help closing the gaps, we are happy to talk it through. No commitment, and no obligation to change who supports you.

And if it is already in good shape, we will tell you that and leave you to it.

INNOVA GROUP

Innova Technologies Group Ltd
Hull, United Kingdom
innovagroup.tech
hello@innovagroup.tech

ALSO IN THIS SERIES

Getting Started with Microsoft 365
Microsoft Copilot Readiness
Making SharePoint Work For You
Cyber Security Essentials Checklist
IT Health Check
Choosing a Technology Partner

STAFF HANDOUTS

Spotting a Phishing Email
Choosing and Using Passwords
Multi-Factor Authentication
Quick Reference Posters

FOUR DISCIPLINES, ONE PARTNER

- **InnovaSystems** — Devices & support
- **InnovaWorks** — Tools that travel
- **InnovaCloud** — Identity & data
- **InnovaSecure** — Access & awareness

Technology That Works. Innovation That Lasts.