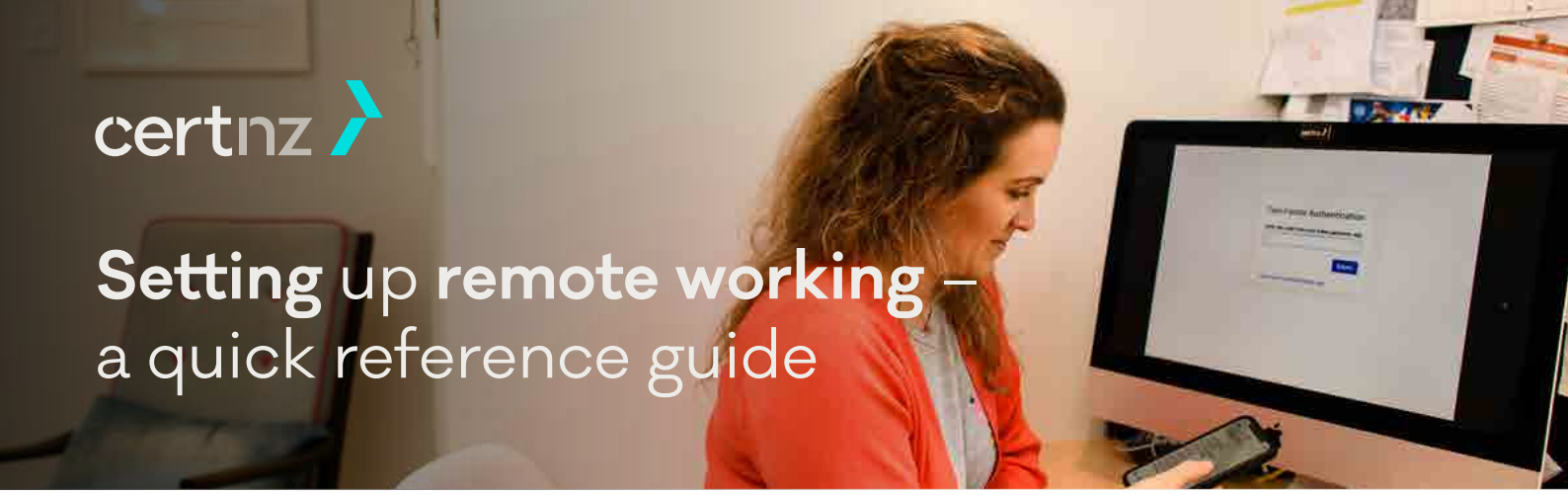

Setting up remote working – a quick reference guide

Working remotely can feel overwhelming if this is something you and your staff are not used to. This quick reference guide walks you through the important steps of setting this up securely. It will help you think about how the business will operate, including helping staff manage their time and set up their remote working space.

You

- [ ] **Make a list of all the important systems your staff need to access in order to carry out minimal business functions.**
  To get started, add your email, team chat and communications, and document storage systems.

- [ ] **Note where those systems can be accessed from.**
  Are they accessed only from within your work office, or can they be accessed from anywhere on the internet (cloud software).

- [ ] **Designate someone as the go-to person to call when there is an incident.**
  Your staff might be used to getting help in person, or having an IT provider they can call. Make it clear who this go-to person is and share their contact information with the team.

- [ ] **Contact CERT NZ if you have an incident.**
  If you have an incident and are unsure what to do, contacting CERT NZ is a great first step. They can help you sift through the facts and head down the right path.

Your network

If you have an office network with important systems:

- [ ] **Pick and configure a remote access software that connects your staff to your office network, like a VPN.**
  Avoid using remote access software that only connects to a user's computer at the office. This will be difficult to manage and will make it hard to control if there was an incident.

- [ ] **Configure the VPN to require two-factor authentication for every user.**
  This is a must-do for every account. This software allows anyone to pretend they are in your office network. It needs to be protected.

- [ ] **Review the VPN throughput and consider if it is enough for your staff.**
  Consider the types of files and sizes they work with. Staff will have to do some work on their local machines, but there will be periods of high traffic which means slower connections.

- [ ] **Configure VPN logging and check them once a week.**
  You want to monitor who is using this digital front door to your office. Configure logs and review them at least once a week to make sure all the traffic appears to be legitimate.

If you have important cloud systems:

- [ ] **Check that two-factor authentication is configured for all accounts.**
  Access to these systems is as important as ever. Protect them from unauthorised access by requiring two-factor authentication.

- [ ] **Check that access logs are configured for all systems.**
  You should review these logs to make sure all access still appears appropriate.

Your staff

- [ ] **Set long, strong, unique passwords to access the VPN.**
- [ ] **Back up any documents they are working on locally (on their device) to the office network or document storage systems.**
  That way you don't have to worry about losing these documents if you lose or break the device.
- [ ] **Check-in with your team regularly (at least daily).**
  Having regular check-ins will allow you know how your staff are doing and if the remote setup is working. It also makes it easier to raise any IT questions or concerns.
- [ ] **Keep any devices or data with you when you are in public spaces.**
  If these devices are at home, it is good to keep up the practice of locking your devices when you are away.

Their devices

- [ ] **Set a long, strong, unique password to unlock any devices.**
- [ ] **Configure devices to download and install software updates automatically.**
  Setting this to happen automatically means you don't have to worry about it.
- [ ] **Configure built-in operating system antivirus and hard-drive encryption software.**
  Microsoft and Apple operating systems build this into their operating systems.
- [ ] **Configure automatic device backups.**
  Although your staff are doing regular uploads of documents back to the network, this is an extra, automatic control for peace of mind.

Find out more at
www.cert.govt.nz/business