# IT Provider audit/checklist

You can use this checklist to frame conversations with your IT provider to ensure that you are getting the best service and advice for your business.

## IT set up

|  | Check that: | Check |
|---|---|---|
| 1 | Your IT provider has expertise in setting up secure IT networks |  |
| 2 | Your IT provider has installed security software (business level antivirus/endpoint protection system) on office computers and on any on site servers |  |
| 3 | As the business owner, you and your IT provider understand the IT security requirements for businesses operating in Health (such as Healthlink and HISF standard etc.) |  |
| 4 | Your IT provider has experience dealing with IT and cyber security incidents |  |
| 5 | You or your IT provider have setup a business domain and secure emailing system for all staff |  |
| 6 | Your IT provider and other IT software/hardware vendors have set up backups for each system and informed you of the backup schedule for each system |  |
| 7 | You have set up policy and processes around how removable media (USB drives) should be used and what information can be copied onto them |  |
| 8 | You or your IT provider have set up an inventory of all IT assets, systems and users and details of what confidential information is held on each |  |
| 9 | Your IT provider has access to information regarding the current IT and cyber security threats and will keep you informed and advise you regarding measures you need to take if your business is likely to be impacted. |  |
| 10 | You choose systems that are secure by design and preferably cloud based (so that you don’t have to pay for additional IT hardware and can run your business anywhere, anytime.) |  |
| 11 | All systems and individuals have strong passwords that are used only by that person, PIN and 2FA for all systems that have the capability. |  |
| 12 | All users have access to systems based on their role. It is not recommended to give all staff the same level of access or full access to all systems/software |  |
| 13 | Your IT provider has a service desk (email, phone) where staff can call in order to get IT Support |  |
| 14 | Your IT Provider provides remote and on-site IT support service |  |

# Day-to-day IT management & support

| | IT actions that will secure your business and patient information | Check |
|---|---|---|
| 1 | Keep all IT software and hardware up-to-date | |
| 2 | Maintain IT asset, systems and users register | |
| 3 | Ensure that the backup of each system is being done as per the schedule established during set up | |
| 4 | Provide regular phishing awareness to all staff | |
| 5 | When a staff leaves their account and access to systems is disabled in a timely manner | |
| 6 | Monitor IT Network for any malicious activity and action accordingly | |
| 7 | Staff access and privileges to use systems is reviewed at regular intervals | |
| 8 | Unused hardware & software are decommissioned | |