IT Check-Up (Quick Self-Assessment)

	Item	Why It Is Important
☐	Do you require employees to log in?	Authentication is an integral part of protecting your company's data. Everyone in your business should have to log in to their computers or the network, ideally as part of a two-factor authentication process. Employees need to be creating unique, strong passwords.
☐	Are you using firewalls?	Having strong hardware- or software-based firewalls helps safeguard your computers and business network from unauthorized access. The firewalls need to be properly configured and regularly updated.
☐	Do you monitor your network?	Monitoring your business network for threats and performance issues is essential. Automated systems are ideal because they can monitor the network in near real- time and notify you when there is a problem.
☐	Are you using security software?	Having security software that scans for different types of malware (e.g., viruses, worms, ransomware, spyware) is important to detect and prevent known threats. It needs to be installed on each computer in your business.
☐	Are employees receiving security training?	Cybersecurity is only as strong as your weakest link. Employees can be the weakest link if they are not properly educated about security issues, such as how to create strong passwords and spot phishing emails.
☐	Is your data being backed up regularly?	Data is a valuable but vulnerable asset. To protect your data, you need to regularly back it up. Equally important, you must make sure the backup files can be successfully restored.
☐	Is the software on your computers up-to-date?	Cybercriminals often exploit known vulnerabilities in software to carry out cyberattacks. Making sure that each computer's operating system and applications have the latest updates can help stop attacks.
☐	Do you have a disaster recovery plan?	A disaster recovery plan (aka business continuity plan) provides detailed information on how to keep essential operations running during an emergency. Having such a plan can minimize losses as well as help your business recover from a disaster.
☐	Are your IT policies up-to-date?	IT policies can help protect your IT assets. Besides traditional IT policies such as an acceptable use policy, you also might need policies addressing modern-day issues, such as social media and Bring Your Own Device (BYOD) policies. Employees need to be informed about all your IT policies.
☐	Do you inventory your IT assets regularly?	Creating a detailed inventory of IT assets keeps track of important information, such as device serial numbers, software installed on devices, and software product keys. Besides being useful during technical support, this information can help identify risks (e.g., security software not installed on a computing device).
☐	Is hardware maintenance performed regularly?	Computers, printers, and other IT equipment periodically need hardware maintenance to avoid problems. For example, cleaning computers' fans and air vents helps keep them from overheating.
☐	Is software maintenance performed regularly?	Computers need routine software maintenance to prevent problems. For instance, clearing out cached and temporary files helps keep the computers from getting too bloated, which can cause performance problems and connectivity issues.