|  |
| --- |
| Business IT Security Checklist |
|  |
| **Strategy and Human Resources Polices** | **Yes** | **No** |
| Do you have a clear IT security policy that’s known to staff? |  |  |
| Do you have policies in place for acceptable technology use, password guidelines and security practices? |  |  |
| Do you have confidentiality agreements for contractors and vendors? |  |  |
| Do you have a privacy policy? |  |  |
| Do you provide regular training to employees about potential security risks and how to avoid them? |  |  |
| **Data Backup** | **Yes** | **No** |
| For critical data (anything needed for day-to-day operations) do you store it on a centralized server and back up nightly? |  |  |
| For critical data (anything needed for day-to-day operations) do you also back it up off-site regularly? |  |  |
| Do you do frequent tests to ensure data is not corrupted and could be restored if necessary? |  |  |
| Do you have technicians or staff members familiar with your network and storage who can restore data quickly if necessary? |  |  |
| **Desktop Security** | **Yes** | **No** |
| Do all computers have working anti-virus software? |  |  |
| Do you have security policies in place for downloading and installing new software? |  |  |
| Do your passwords have a minimum of 8 alphanumeric characters? |  |  |
| Do you require employees to use 2-factor authentication? |  |  |
| Are all computers updated with the latest system updates and security patches? |  |  |
| Do you have a way to keep track of who is given access to passwords? |  |  |
| Are you able to retrieve employee passwords if necessary? |  |  |
| Are your operating systems, web browsers and software up-to-date? |  |  |
| Are patches deployed quickly when necessary?  |  |  |
| **Internet and Network Security** | **Yes** | **No** |
| Do you have a firewall and intrusion detection on all web connections? |  |  |
| Do you use a Virtual Private Network (VPN) for remote access? |  |  |
| Are all modem and wireless access connections known and secure? |  |  |
| Do you monitor you network in real-time so you are instantly able to identify threats? |  |  |
| If you identify a threat, do you have a staff member who is able to address the threat immediately? |  |  |
| **Privacy and Sensitive Information** | **Yes** | **No** |
| Is customer financial/personal/health information encrypted and accessible only to those who need it? |  |  |
| Are paper files kept in locked filing cabinets with controlled access? |  |  |
| **Audit** | **Yes** | **No** |
| Do you do a periodic audit of your IT security checklist (at least every 6 months)? |  |  |
| If you find gaps in your policies, do you have the financial and talent resources to fix them quickly? |  |  |