Endpoint Security Checklist

Every laptop and workstation is a possible way in

Your devices are the front line. Use this to find the weak ones before someone else does.

		YES	NO
1.	Are all business devices actively monitored, including remote and traveling ones?	☐	☐
2.	Are operating systems and software kept current on every device?	☐	☐
3.	Is EDR or MDR in place and actively watched?	☐	☐
4.	Are local administrator rights restricted?	☐	☐
5.	Are lost or stolen devices encrypted to protect company data?	☐	☐
6.	Do you control whether personal devices can access business data?	☐	☐
7.	Are remote employees protected to the same standard as office employees?	☐	☐
8.	Do you have a complete inventory of every device that touches company data?	☐	☐
9.	Can a compromised device be isolated quickly before an attack spreads?	☐	☐
10.	Are endpoint security alerts reviewed and acted on by a qualified team?	☐	☐
11.	Are staff trained to verify downloads from search results, AI answers, and unfamiliar links?	☐	☐
12.	Are only approved applications allowed to run on company devices?	☐	☐
13.	Are servers protected and monitored like laptops and workstations?	☐	☐
14.	Are phones and tablets protected when they access email, files, or business apps?	☐	☐
15.	Can company data be remotely wiped from lost, stolen, or former employee devices?	☐	☐
16.	Are USB drives and removable storage devices controlled or restricted?	☐	☐
17.	Is every new device securely set up before it is given to an employee?	☐	☐
18.	Is there a process to remove access, wipe data, and recover devices when employees leave?	☐	☐
19.	Are file recovery options in place for critical devices?	☐	☐
20.	Are device security settings reviewed regularly, not just at setup?	☐	☐

Why this matters: It only takes one unprotected device to give an attacker a way into everything.

Use this checklist to make sure your laptops and workstations are not your weakest link.

Need help? Contact us.

mytampait.com | (813) 513-9849 | sales@mytampait.com