New Employee Cybersecurity Checklist

Password Power

- □ I've created a strong, unique password for each system I access
- □ I'm using multi-factor authentication (MFA) when available
- □ I never reuse passwords across different platforms
- □ I don't store passwords on sticky notes or visible places

Phishing Patrol

- □ I can recognize phishing emails and suspicious links
- □ I know not to click unexpected attachments or links
- □ I verify sender addresses before acting on email requests
- □ I know what to do if I accidentally click on something sketchy

Device & Screen Safety

- □ I always lock my screen when stepping away
- □ I never leave sensitive information visible at my workstation
- □ I know how to secure my mobile devices if I use them at work
- □ I avoid using public Wi-Fi for any work-related tasks

Internet Smarts

- □ I go directly to websites, not through random search results
- □ I avoid downloading software or files unless it's approved by management
- □ I report suspicious pop-ups or website behavior immediately

Know the Plan

- □ I know who to contact for IT or security issues
- □ I understand the practice's incident response steps
- □ I know how to report a possible cyber threat
- □ I feel comfortable asking questions about anything unclear

Security Is a Team Sport

- □ I feel confident in my role as part of the cybersecurity team
- □ I understand that protecting patient data is part of my daily job
- □ I'm committed to keeping learning as threats evolve

Pact-One Solutions | pact-one.com | 866-722-8663