rightworks

rightworks.com

Bookkeeper Cloud Security Checklist

Where are you most vulnerable? Let's find out.

Your clients trust you with their most sensitive data. This checklist highlights the essential safeguards bookkeeping firms need to keep client trust, stay compliant, and avoid IT headaches.

	Put "1" next to every tool your SaaS setup already has 👇	
Access and Identity Control	Secure single sign-on	
	Centralized app access	
	Credential masking	
	Multifactor authentication (MFA)	
User Management and Oversight	One-click user offboarding	
	Login tracking and audit logs	
	Role-based permissions	
Device and Endpoint Security	24/7 threat monitoring	
	Automatic OS/browser updates	
	Secure Wi-Fi & firewall protection	
Human Security Awareness	Ongoing staff training	
	Phishing simulations or alerts	
	Suspicious email response policy	
	Lost/stolen device procedure	
AI and Productivity Tools	Private AI chat for secure tasks	
	Approved AI tools only (no client data in public models)	
Support and Compliance Readiness	24/7 accounting-trained helpdesk	
	Written Information Security Plan (WISP)	
	Audit log retention	
	Secure office network & device policy enforcement	
	Total	**0 /20**

Add your numbers to get your score.

16–20: You're in great shape! Consult a security pro to make sure your tools can grow with you.

10–15: You're in decent shape. But even one vulnerability can lead to big risks. We can help.

0–9: It's time to act. Get in touch to learn how we can protect your clients, your data, and yourself, ASAP.

Check off "security" in one fell swoop.

Rightworks manages your security so you can balance books, not IT.

GET STARTED >>