Integris.

DIY IT SECURITY AUDIT CHECKLIST

Learn how secure your business is, and how to make it safer.

All Network Devices	YES	NO	IN PROGRESS	NOTES:
Are all unused ports disconnected?				
Are all devices using a password protected Wi-Fi connection?				
Are all of your apps, firmware, upgrades, patches and updates from trustworthy sources?				
List of all devices, types, serial numbers, locations, and security upgrade status (Download the Asset Tracking Spreadsheet)				
Are BYOD policies covered under an acceptable use policy and a Mobile Device Management platform? (Sample BYOD Policy)				
Are all devices using standard configuration to maintain manageability?				
Is your network using SNMPv3 (if using a simple network management protocol)?				
Are your devices purchased from trustworthy sources?				
Are there procedures in place to report and disconnect lost or stolen devices?				

Patch Management Strategy	YES	NO	IN PROGRESS	NOTES:
Does your IT department have a patch management solution?				
Do all users understand that patches and updates must be done as quickly as possible?				
Have all unsupported software or applications on any devices accessing our network have been removed or disabled?				
Is your software licensed with security patches enabled?				

Firewall	YES	NO	IN PROGRESS	NOTES:
Do you have a firewall in place to keep unauthorized parties out of your network?				
Have you had a professional or authorized administrator approve and document every firewall rule?				
Do you require authentication for securing your routing protocols?				
Have you changed your firewall password from its defaut to a stronger one?				
Do you have steps in place for documenting and investigating alerts?				
Are all unnecessary firewall permissions and rules disabled?				
Are all firewall settings for access lists, outbound and inbounded, set for "Deny All"?				

Malware Protection	YES	NO	IN PROGRESS	NOTES:
Does your antivirus include an email filter?				
Does your antivirus scan web pages, files and applications routinely to spot and block malware?				
Every device, both workstation and mobile, has updated anti-malware protections in place.				

User Responsibility	YES	NO	IN PROGRESS	NOTES:
Is remote access limited to just those who specifically need it?				
Is there documentation of all users and their privileges available?				
Do you have a rigid password policy, including numbers, special characters, length and capitalization rules?				
Is 2-factor authentication (2FA) in place for all users?				
Is each user name unique with no relation to his or her actual name or email account?				
Do you have a policy in place for immediately revoking user permissions and access for users who leave your company?				
Remote access limited to just one approved method?				
Have your employees completed a basic cybersecurity awareness training class?				
Does your organization have a VPN for remote access of devices?				
Is your public Wi-Fi separated from your employee Wi-Fi?				
Do your employees lock completely out of all devices when they are finished working?				
Are your users following password best practices?				

Email and Internet Security	YES	NO	IN PROGRESS	NOTES:
Are you using a spam filter to block spam, phishing and malware on outbound as well as inbound traffic?				
Do you have an internet security platform that performs DNS filtering and dark web monitoring?				
Are all platforms, software, files and applications scanned by your anti-malware?				
Are all avenues for users to bypass your security solution blocked?				
Are your devices set up to avoid directory harvesting attacks? (DHAs)?				

Internal IT Department Responsibility	YES	NO	IN PROGRESS	NOTES:
Is all data backed up and tested for functionality of the backups?				
Do they require all mobile and remote devices to be encrypted?				
Do they routinely and randomly check the status of patches and updates on workstations and all devices?				
Does your IT department work with your HR to establish policies for onboarding, acceptable use policies, and cyber awareness training for new employees.				
Is the Universal Plug-n-Play option disabled?				
Is your organization's file sharing default option "Read Only" with completed control to edit given to administration?				
Do they routinely perform penetration testing, phishing simulations, and other tests to determine vulnerabilities?				
Do you have an acceptable use policy signed and on file for everyone who accesses your network?				
Is WPS (wireless protected setup) disabled on mobile and wireless devices?				
Are devices set with automatic inactivity log-outs?				
Are backups stored separately from the main network?				
Is 2-factor authentication (2FA) in place for all users?				

Cyberthreat Landscape	YES	NO	IN PROGRESS	NOTES:
What are the trending cyberthreats for your vertical?				
What would a disruption of your network cost you in lost productivity, mitigation, and restoration? (Use our Downtime Calculator)				
Are third-party vendors limited in their ability to access only required data?				
What part of your network is most vulnerable to cyberattacks?				
What is the likelihood that an identified cyberthreat would succeed?				
What are the ways each cyberthreat you have identified could impact your business?				
What cyberthreats have your peers experienced, and were they successful?				
How much damage would the recognized cyberthreats do to the network and your devices?				

Physical Device Security	YES	NO	IN PROGRESS	NOTES:
Do you have physical security features in place? (keycards, locks, etc.)				
Are your Operational Technology devices (such as heating controls and lighting) protected?				
Are your IOT devices and machines protected or on a separate network?				
Do you have tracking software in place on devices in case they are lost or stolen?				

Contact us at **sales@integrisit.com** or **integrisit.com/contact**