

TECHNOIDS TECHNOLOGY SECURITY REVIEW SERIES

Education & Workforce Technology Security Checklist

A practical review worksheet for training labs, shared computers, accounts, wireless, grant-funded equipment, recovery, and lifecycle planning.

YES / NO / NOT SURE / N/A

This is not a pass/fail cybersecurity test.
A No or Not Sure identifies an area worth understanding more closely.

Technoids Techs

Knowledge Is Part of Protection.

Digital Technology. Real-World Care.

Education & Workforce Technology Security Checklist

Knowledge Is Part of Protection. Use this worksheet to review the technology and security areas that commonly matter to education, workforce development, and training organizations: training labs, shared devices, accounts, wireless networks, trainee/student information, program technology, grant-funded assets, backup and recovery, and lifecycle planning.

How to use this checklist	Review each question and mark the answer that best reflects your current visibility. The goal is not to score your organization. The goal is to identify what you understand, what may need attention, and what would be useful to discuss with Technoids Techs.	
Organization _____ _____	Completed by _____	Date _____

YES	A control or process appears to exist.
NO	An area may deserve further evaluation.
NOT SURE	An area where visibility may be missing.
N/A	Not applicable to your environment.

This is not a pass/fail cybersecurity test. A No or Not Sure identifies an area worth understanding more closely.

Training Environment

Review question	YES	NO	NOT SURE	N/A
Do we maintain an inventory of all training computers?				
Do training computers use a standardized configuration?				
Can trainees make administrative changes to shared computers?				
Is there a process for preparing/resetting computers between classes?				
Are required training applications centrally managed?				
Do we know which computers are approaching replacement?				

Accounts & Access

Review question	YES	NO	NOT SURE	N/A
Do trainees have appropriate individual or controlled accounts?				
Are instructor accounts separated from trainee access?				
Are administrative systems restricted from trainees?				
Are unused accounts removed?				
Is MFA enabled for employee/administrative accounts?				
Are privileged accounts restricted?				

Network & Wireless

Review question	YES	NO	NOT SURE	N/A
Is the training network separated from administrative systems where appropriate?				
Is guest Wi-Fi separated from internal resources?				
Is employee wireless appropriately secured?				
Has wireless capacity been evaluated for expected device density?				
Is the firewall actively managed?				
Are infrastructure/IoT devices appropriately segmented where necessary?				

Security & Information

Review question	YES	NO	NOT SURE	N/A
Are shared computers regularly patched?				
Are endpoints protected by managed security tools?				
Is email protected against phishing?				
Do we know where trainee/student information is stored?				
Is administrative information separated appropriately?				
Are employees trained to recognize cybersecurity threats?				

Program & Grant Technology

Review question	YES	NO	NOT SURE	N/A
Are grant-funded technology assets inventoried?				
Do we understand licensing costs after funding ends?				
Is there an ongoing support plan for funded equipment?				
Have replacement costs been considered?				
Is technology planning included when new training programs are developed?				

Recovery & Lifecycle

Review question	YES	NO	NOT SURE	N/A
Is critical organizational information backed up?				
Are backup failures monitored?				
Has recovery been tested?				
Do we have a process for cybersecurity incidents?				
Do we maintain a technology replacement roadmap?				
Do we budget for equipment lifecycle instead of waiting for failure?				

What Did You Discover?

This checklist is not designed to give your organization a cybersecurity grade. Technology environments are too different for a simple score to tell the entire story. Instead, look at your answers and use them to guide the next conversation.

YES	_____	NO	_____
NOT SURE	_____	N/A	_____

How to Interpret Your Answers

YES	A control or process appears to exist.
NO	An area may deserve further evaluation.
NOT SURE	An area where visibility may be missing.
N/A	Not applicable to your environment.

Do not start with the product. Start with the questions: What are we protecting? Who has access? Which technology do we depend on? Where are our largest risks? What do we not know? What should we address first?

Areas I Want to Review

1. _____
2. _____
3. _____

Questions for Technoids Techs

1. _____
2. _____
3. _____
4. _____

Want Help Reviewing Your Answers?

Bring your completed checklist to a Technoids Technology & Security Review. We'll help you understand what your answers may mean, which areas deserve closer attention, and what practical next steps may make sense for your organization.

Schedule a Technology & Security Review

Technoids Techs

Knowledge Is Part of Protection.

Digital Technology. Real-World Care.

Practical managed technology, cybersecurity, compliance support, and planning for organizations where digital systems affect real people, real responsibilities, and real operations.

Educational-use disclaimer: This checklist is provided for general educational purposes and is not a certification, audit, legal opinion, regulatory determination, or guarantee of cybersecurity or compliance. Organizations should consult appropriate legal, regulatory, insurance, or compliance advisors for requirements specific to their situation.