District Security Checklist

What is your district's state of security readiness? *Security means reliability and integrity of the operation as well as keeping the door locked on data. Use this questionnaire to gain a quick sense of your overall security profile. Then get a more in-depth analysis by using the District Security Rubric and Planning Grid to pinpoint areas of concern and identify next steps.*

You can fill out this checklist on line and have your score automatically computed for you. Or you can print it and do it

District Demographics

My District is: __ Urban Suburban Rural __ Other

Our student population is: <1,000 1,000-2,000 2,000-5,000 5,000–10,000 >10,000

Our percentage of students eligible for free or reduced lunch is:

__ < 20% 20%-40% 40%-60% 60%-80% > 80%

How to score your answers: If your answer to a question is an unqualified 'yes', give yourself the maximum point value for that question. If your answer is 'maybe' or 'half done' or 'almost', give yourself appropriate partial credit up to the maximum point value for that question. A definite 'no' rates a zero. Maximum score is 100 points.

A. Management (25 pts)

District Goals, Policy and Support (5 pts)	Max Pts	Your Score
Does your district have clearly stated educational goals and values that guide security decisions and connect security practices to teaching & learning priorities?	2	
Do district policies address data confidentiality and personal privacy in compliance with laws, regulations, and community expectations?	2	
Does the district budget allocate funds to support security including personnel, hardware and software?	1	

Security Management Implementation (5 pts)	Max Pts	Your Score
Is there a Security Team authorized by the district cabinet that meets on a scheduled basis to discuss security planning and oversight?	1	
The superintendent (or a representative of the school board or school committee) is included on the security team to ensure community standards are met?	1	
Security team verifies full compliance with all State and Federal Laws. Compliance review is routine component of new installations and periodic review.	2	
There are clearly documented procedures in place that include how to report and document security issues, and steps for response and follow up.	1	

Security Planning and Preparedness (15 pts)	Max Pts	Your Score
Security Plan: Does the district have a security plan that has been significantly reviewed and updated in the past 12 months?	2	
Security Insurance: Has the district completed a cost/benefit analysis for security insurance, updated in the past 12 months?	1	
Scope of Plan: Does the scope of the Security Plan include		
▸ Benchmarks for the immediate and long-term improvement of both perimeter and internal defenses?	1	
▸ Needed improvements in operations, *e.g.* maintenance, backup, and system monitoring?	1	
▸ User involvement in setting policies and methods for regular user feedback about security and other operational issues?	1	
▸ User training and communication, as well as regular communications with other stakeholders?	1	
Security Audit: Have the district's security operations been reviewed or audited by an outside group within the past two years an and internal audit annually?	1	
▸ If an audit was completed, have the auditors' recommendations been fully implemented?	1	
Security Penetration Test: Have the district's security operations been penetration tested by an outside group within the past two years an and internal audit annually?	1	
▸ If a penetration test was completed, have the testers' recommendations been fully implemented?	1	
Staffing: Are staffing levels sufficient to…		
▸ Complete routine network management tasks?	2	
▸ Complete all security-related tasks regularly?	1	
▸ Provide customer service at appropriate levels?	1	

B. Technology (50 pts)

Perimeter Defenses (15 pts)	Max Pts	Your Score
Does your network design isolate web and email servers in a semi-isolated area commonly referred to as a DMZ?	2	
Is the network perimeter protected by a spam/content filter?	1	
Do the firewall/multifunction devices include virus protection?	2	
Is spam, content, and virus protection enabled on email and web servers?	2	
Is your IPS properly configured and fully functioning to monitor critical facilities?	1	
Are all wireless access points fully encrypted (to WPA standards, or better)?	2	

Are perimeter defenses regularly tested for vulnerability to penetration?	1	
Are web filters in place to comply with legal requirements, with the ability for authorized overrides?	1	
Is your VPN configured to provide secure access to all authorized remote users?	1	
Are perimeter defenses regularly tested for vulnerability to penetration?	2	

LAN Management (15 pts)	Max Pts	Your Score
Do you have live monitoring for network intrusion and virus protection?	2	
Is the network fully documented, and is the equipment inventory up to date?	3	
Are all critical servers are protected by redundant units?	2	
Standardization and Redundancy: Do you have the capacity to swap out defective equipment?	2	
External Partners and Vendors: Have you validated the effectiveness of the data privacy and intrusion security capabilities of all outside parties with whom you share data or from whom you receive services (e.g. payroll, email, webhost, ISP, etc)?	2	
Are Backups		
Performed regularly?	1	
Tested routinely?	1	
Centrally Managed?	1	
Stored offsite ?	1	

WAN Management (20 pts)	Max Pts	Your Score
Maintenance and Monitoring Protocols:		
▸ network monitoring of bandwidth, connections, and file types	1	
▸ routine preventive maintenance of desktops, LAN servers, network appliances	2	
▸ scheduled testing of network performance	1	
Remote Management: Do you have the capacity to remotely rebuild desktops, and monitor, update or reset LAN servers/routers from a central location? Are key staff automatically notified 24/7 by phone and/or email if a problem occurs?	2	
Segmentation: Are computer connections on your network logically organized by building, department or other hierarchical structure?	2	
Patch and Virus Management: Is virus protection software installed and automatically updated on every workstation?	2	
▸ Are software vulnerabilities patched routinely on all workstations?	1	
▸ Add an additional point if patched automatically.	1	
External Partners and Vendors: Have you validated the effectiveness of the data privacy and intrusion security capabilities of all outside parties with whom you share data or from whom you receive services (e.g. payroll, email, webhost, ISP, etc)? Do vendor passwords follow district policy with respect to complexity, strength, and longevity?	1	
Encryption: Is all student, employee and financial data is encrypted in storage and in transit?	2	
Cloud Security: Are contracts structured so that security is accounted for? Contract delineates full division of responsibility between district and CSP Contract or SLA includes Event logging and notification • DDOS protection • Availability requirements • Intrusion detection and prevention • Data ownership • Data security • Compliance with legal and policy requirements of the district Contract specifies that data is returned to the district and wiped everywhere when the district concludes their contract.	1	
Passwords: Is there a district-wide authentication and authorization policy in place and actively enforced?	2	
▸ *If all computers are password protected, give yourself 1 point.*	1	
▸ *If passwords must be changed periodically, give yourself point.*	1	

Cloud Security: Are contracts structured so that security is accounted for?	1	
Passwords: Is there a district-wide authentication and authorization policy in place and actively enforced?	2	
▸ *If all computers are password protected, give yourself 1 point.*	1	
▸ *If passwords must be changed periodically, give yourself point.*	1	

C. Business Continuity (15 pts)

IT Crisis Management Plan (7 pts)	Max Pts	Your Score
IT Crisis Management Plan: Do you have an asset based model that includes details of all systems that is reviewed and updated annually?	2	
Inventory and Redundancy: Does the plan include complete assessment of inventory and required redundancies of equipment and personnel?	1	
Training: Are personnel trained for Crisis situations including simulations?	1	
Crisis Management: Has a crisis management/operational continuity plan been written or updated within the past 2 years?	1	
Training and Testing: Have staff members practiced implementing the crisis management plan in the past year, and then revised the plan based on that experience?	1	

Environmental Safety (4 pts)	Max Pts	Your Score
Environmental Disasters: Is your network infrastructure located and installed in an area protected from floods, hurricanes, tornadoes, or other regionally-relevant natural threats?	1	
Fire Protection: Are network servers protected by appropriate alarms and fire suppression equipment?	1	
Temperature and Humidity Control: Is network equipment properly ventilated?	1	
Power: Are all servers and network devices protected by uninterruptible power supply (UPS) devices?	1	
Ransomware: Are all devices backed up in order to be able to restore from ransomware incidents	1	

Physical Security (4 pts)	Max Pts	Your Score
Secure Locations: Are all network devices located in secure facilities exclusively dedicated to network operations?	1	
Secure Infrastructure: Are all switches, hubs, and wiring closets located in spaces not also used by custodians, librarians, etc.?	1	
Equipment Security: Is all equipment located in high-use areas secured to prevent theft?	1	
Access Control: Are computer facilities accessible to students and staff only under controlled circumstances (ID cards, entry logs)?	1	

D. Stakeholder/End User (10 pts)

User Engagement and Stakeholder Communication (10 pts)	Max Pts	Your Score
Training: Is training done in a manner most convenient to users to increase user skill and understanding about security procedures, passwords, etc?		
▸ Has a majority of users participated in these sessions?	1	
Communication: Are updates on technology and security regularly sent to stakeholders using email, newsletters, posters, and public media?	2	
Feedback: Is there a help desk to track problems and suggestions? Are there regular electronic and face-to-face forums for user feedback, suggestions, and complaints? Is feedback respectfully listened to and acted upon?	1	
Summary: Have you created a "community of trust" in which users take responsibility for their role in security and also feel that their rights are respected and needs addressed?	2	
Awareness: Do leaders demonstrate competency and knowledge of strategic security practices? Do users integrate essential security practices in use of technology	2	
Access Control: Is staff and student access to technology controlled as needed and restricted as appropriate?	2	

If your district scores:

Below 20:	Either your district doesn't use IT to any significant degree, or your system is a disaster waiting to happen.
20 to 39:	Your district's IT system is probably barely meeting the minimal basic security, but serious shortcomings remain and problems are likely to occur.
40 to 59:	Your district's IT system is beginning to deal with the wide range of security requirements, but continued attention and effort will be needed to bring things up to a more defendable state.
60 to 79:	Your district's IT system is grappling with the wide range of security requirements, and while that does not guarantee no problems will occur, you are exercising appropriate due diligence; however, some shortcomings remain and continued attention and effort will be helpful.
80 to 100:	Your district's IT system is a model of good cyber security practice. Maintaining this status will require continuing attention and action.