Security Audit Checklist

Cybersecurity Self-Assessment Checklist

School Name: _____

Assessment Date: _____

Completed By: _____

Instructions

For each item, mark: **Yes** (2 pts) | **Partial** (1 pt) | **No** (0 pts)

This checklist covers fundamental security controls. A professional assessment may identify additional issues.

Section A: Access Controls (20 points possible)

#	Control	Status	Notes
A1	Multi-factor authentication (MFA) enabled for ALL staff email accounts	Yes / Partial / No	
A2	MFA enabled for all administrative systems (SIS, HR, finance)	Yes / Partial / No	
A3	Password policy enforced (minimum 12 characters, complexity required)	Yes / Partial / No	
A4	Terminated employee accounts disabled within 24 hours	Yes / Partial / No	
A5		Yes / Partial / No	

#	Control	Status	Notes
	Privileged/admin access limited to those who need it		
A6	Admin accounts are separate from daily-use accounts	Yes / Partial / No	
A7	Vendor/contractor access reviewed and revoked when not needed	Yes / Partial / No	
A8	Guest network completely isolated from internal network	Yes / Partial / No	
A9	Student accounts have appropriate access restrictions	Yes / Partial / No	
A10	Service accounts documented, audited, and using strong credentials	Yes / Partial / No	

Section A Score: _____ / 20

Section B: Network Security (16 points possible)

#	Control	Status	Notes
B1	Firewall configured with documented rules	Yes / Partial / No	
B2	Network segmented (separate VLANs for students, staff, admin, IoT)	Yes / Partial / No	
B3	Wireless networks use WPA3 or WPA2-Enterprise	Yes / Partial / No	
B4	Remote access requires VPN or zero-trust solution	Yes / Partial / No	
B5	DNS filtering blocks known malicious domains	Yes / Partial / No	
B6	Web content filtering appropriate for educational setting	Yes / Partial / No	
B7	Network traffic monitored for anomalies	Yes / Partial / No	
B8		Yes / Partial / No	

#	Control	Status	Notes
	Public-facing services minimized and secured		

Section B Score: _____ / 16

Section C: Endpoint Security (12 points possible)

#	Control	Status	Notes
C1	Antivirus/EDR installed and active on all endpoints	Yes / Partial / No	
C2	Automatic updates enabled for operating systems	Yes / Partial / No	
C3	Automatic updates enabled for applications	Yes / Partial / No	
C4	Full-disk encryption enabled on all devices (BitLocker, FileVault)	Yes / Partial / No	
C5	Mobile device management (MDM) deployed for school devices	Yes / Partial / No	
C6	End-of-life systems identified and isolated or replaced	Yes / Partial / No	

Section C Score: _____ / 12

Section D: Data Protection (12 points possible)

#	Control	Status	Notes
D1	Backup system in place for critical data	Yes / Partial / No	
D2	At least one backup copy stored offline or air-gapped	Yes / Partial / No	
D3	Backup restoration tested within the last 90 days	Yes / Partial / No	
D4	Sensitive data identified and classified	Yes / Partial / No	
D5	Data retention policies documented and followed	Yes / Partial / No	

#	Control	Status	Notes
D6	Secure data disposal procedures in place	Yes / Partial / No	

Section D Score: _____ / 12

Section E: Email Security (10 points possible)

#	Control	Status	Notes
E1	SPF record configured correctly	Yes / Partial / No	
E2	DKIM signing enabled	Yes / Partial / No	
E3	DMARC policy configured (reject or quarantine)	Yes / Partial / No	
E4	External email warning banner displays for external senders	Yes / Partial / No	
E5	Phishing simulation conducted within the past year	Yes / Partial / No	

Section E Score: _____ / 10

Section F: Policies & Procedures (10 points possible)

#	Control	Status	Notes
F1	Acceptable use policy current and communicated annually	Yes / Partial / No	
F2	Incident response plan documented and accessible	Yes / Partial / No	
F3	Security awareness training conducted annually for all staff	Yes / Partial / No	
F4	Vendor security requirements documented in contracts	Yes / Partial / No	
F5	Cyber insurance coverage adequate and policy current	Yes / Partial / No	

Section F Score: _____ / 10

Scoring Summary

Section	Your Score	Maximum
A: Access Controls		20
B: Network Security		16
C: Endpoint Security		12
D: Data Protection		12
E: Email Security		10
F: Policies & Procedures		10
TOTAL		**80**

Scoring Guide

Score Range	Assessment	Recommended Action
70-80	Strong security posture	Focus on continuous improvement and emerging threats
55-69	Solid foundation with gaps	Address high-priority items within 90 days
40-54	Significant vulnerabilities	Create remediation plan; consider professional assessment
Below 40	Critical risk	Immediate action needed; engage security professional

Priority Remediation Guide

If you can only address 5 things, do these first:

1. **Enable MFA everywhere** (A1, A2)
   - Stops 99%+ of credential-based attacks
   - Start with admin accounts, then all staff
2. **Verify your backups work** (D1, D2, D3)
   - Test an actual restore, not just the backup job
   - Ensure at least one copy is offline/air-gapped
3. **Patch critical systems** (C2, C3)
   - Enable automatic updates where possible
   - Prioritize internet-facing and email systems
4. **Train your staff** (F3)
   - Annual security awareness training
   - Phishing simulations to reinforce learning

5. **Create an incident response plan** (F2)
    - Know who to call before you need to
    - Print copies - they may be inaccessible during an attack

---

Items Requiring Immediate Attention

List any items scored “No” that represent critical vulnerabilities:

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

Remediation Plan

Item #	Issue	Action Required	Owner	Target Date	Status

Next Assessment Date:

_____

Notes

_____

Approval

Assessment Reviewed By: _____

Title: _____

Date: _____

Signature: _____

This self-assessment template is provided by AISL (AI for St. Louis Schools). It is not a substitute for a professional security assessment. Reassess quarterly to track improvement.