SAMPLE DATA SECURITY SELF-ASSESSMENT

Based on Strive Together's Student Data Privacy Best Practices[1]

Use this checklist to measure your organization's readiness to work with individually identifiable student data. For each checklist item, rate your organization's current status. At the end of the checklist, there is space to set up to three goals for data security improvement.

DATA SECURITY CHECKLIST

Guiding Principle: *Organizations respect student privacy by employing strong administrative, technical, and physical data security strategies to guide against breaches and unauthorized use*

ADMINISTRATIVE SECURITY: CONTROLLING WHO CAN ACCESS AND HOW	IN PLACE? (YES/NO/UNSURE)
We limit user access to student data by establishing and safeguarding individual logins	
We regularly delete user accounts that are no longer in use	
TECHNICAL SECURITY: PROTECTING FILES AND RECORDS IN YOUR COMPUTER	**IN PLACE? (YES/NO/UNSURE)**
We encrypt all data in motion (transmitted over secure connections) and at rest (inactivity)	
Our network is protected by firewalls and/or network address filtering	
PHYSICAL SECURITY: PROTECTING THE MACHINES THAT HOLD RECORDS	**IN PLACE? (YES/NO/UNSURE)**
Data is not stored on local workstation, but is on a designated secured machine	
All physical media where data is stored are physically protected	
We shred or securely delete participant data that is no longer needed	
OVERALL SECURITY	**IN PLACE? (YES/NO/UNSURE)**
We have designated a "chief security officer"	
We have cyber liability insurance and require it of vendors	
We have conducted security audits and require vendors to do the same	
We have protocols in place to deal with any potential security breaches	

[1] Strive Together (2014). Student Data Privacy: Best Practices. Retrieved from https://www.strivetogether.org/wp-content/uploads/2017/04/student-data-privacy-best-practices.pdf

GOAL SETTING

Based on the above self-assessment, what are goals that you have around data security? Be as specific as possible (e.g. "Designate an internal point person for data security and create a written description of the responsibilities involved in this role").

1.

2.

3.

.