DATA SENSITIVITY[1] AND REVIEW FRAMEWORK FOR EVALUATING PRIVACY AND SECURITY SAFEGUARDS IN CLOUD AND HOSTED SERVICES

This guidance is a starting point, but not a complete substitute, for a case-by-case analysis.

HIGH SENSITIVITY

Data	Review Procedure
Personally identifiable information. Types: • **SSN** • **Credit card, debit card, or bank account number** • **Other data requiring notification in event of breach** • **Certain health information (treatment, diagnosis, certain care settings)** • **Certain student records (final grades, disciplinary, academic materials)** • **Certain HR records (salary, performance review, disciplinary)** • **Certain alumni data (giving, contact reports)** • **Other personal, highly sensitive data**	**Legal. Require contract with strong privacy and security requirements (*Purchase Order Exhibit A* contents in agreement itself). Consider need for FERPA, HIPAA, PCI, subcontractor, security assurances language. AND**
	Due diligence of security practices. Examples: • **SAS 70 Type II or ISO 27001 certification** • **Alternate third party certification based on recognized security controls** • ***SPIA for Vendors* that is reviewed and accepted by information security and privacy personnel** • **Other detailed security program documentation reviewed and accepted by information security and privacy personnel**
	Additional Risks and Mitigation. **Based on discussion/reviews, there may be additional steps necessary to address privacy and security concerns.** **For example, Penn may ask for the elimination or reduction in SSNs, for encryption of certain highly sensitive data, for compensating security controls, limitations on or opt-outs on marketing communications.**

MEDIUM SENSITIVITY

Data	Procedure
Personally identifiable information. Types: • **Contact information** • **All FERPA-protected information that is not included in High Sensitivity category** • **Other personal, but not highly sensitive data**	**Legal. Require contract or purchase order with strong privacy and security requirements (*Purchase Order Exhibit A* contain such language) AND**
	Due diligence of security practices. Examples: • **Any of the above** • **Review of Terms of Use and Privacy Policies by security or privacy personnel (Note whether Terms specify that they can be changed at any time)**

[1] Data sensitivity is based on type of data, degree of identifiability, complexity of data sharing.

	<u>Additional Risks and Mitigation</u>. **Based on discussion/reviews, there may be additional steps necessary to address privacy and security concerns.** **For example, Penn may ask for compensating security controls or limitations on or opt-outs on marketing communications.**

LOW SENSITIVITY

<u>Data</u>	**<u>Procedure</u>**
Data very unlikely to be identifiable or, if identifiable is broadly public information	• **Review of Terms of Use and Privacy Policy (Note whether Terms specify that they can be changed at any time)**