These instructions are recommended for use by CSU Buyers and/or Contract Administrators only. *Do not simply attach the Supplemental Provisions (Rider A) to the CSU General Provisions for Information Technology Acquisitions.* Review the Supplemental Provisions in its entirety for content and applicability. Sections 1.0 to 9.0, respectively, sets forth the “use” and “purpose” for each section. Buyer/contract administrator will need to select the appropriate sections that relate to your contract. The Supplemental Provisions were created to be used as a tool to comply with CSU Information Security Requirements, and may be modified as needed subject to the approval of the Procurement Director or Campus Information Security Officer.

**Section I.** If the product/service involves CSU Protected Data, or if the Contractor has access to or stores protected data, select one or more of the following provisions that apply:

1.0  Acknowledgement  
2.0  Disclosure Requirements  
3.0  Information Security Plan  
4.0  Incident Response Management  
5.0  Compliance  
6.0  Personnel Security Requirements  
7.0  Record Retention Requirements  
8.0  CSU right to conduct and/or review risk assessments  
9.0  Terminating or expiring the agreement – return/destroy protected data

**Section II.** If the product/service pertains to Section I, and/or involves payment card data, credit card data, or ACH payments, select one or more of the following provisions that apply:

5.1  PCI-DSS Requirements  
5.2  PA DSS REQUIREMENTS  
5.3  NACHA Requirements

**Section III.** If the product/service pertains to Section I, and/or involves patient health information, select the following provision:
5.4 Health Insurance Portability and Accountability Act (HIPAA) Requirements. (In some cases, a Business Associate Agreement will be required and submitted as an attachment to this provision.)