**PCI 3rd Party Service Provider Check List**

|  |  |  |
| --- | --- | --- |
| **Items that need to be completed** | **Description** | **Completed** |
| * IT SRQ / Campus IT review
 | Custom built for each new 3rd party |[ ]  YES |[ ]  NO |  |  |
| * Acknowledgement from 3rd party per **PCI DSS 12.8.2**
 | 3rd party must present us their acknowledgment or they need to sign our [3rd party agreement](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Service_Provider_Agreement.docx?d=wb1504dc4d92b4e1ebab36db1aea924ab) |[ ]  YES |[ ]  NO |  |  |
| * Attestation of Compliance (AOC) or other PCI compliance review per **PCI DSS 12.8.4**
 | See [University Credit Card Policy](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Credit_Card_Policy.docx?d=we18ee794de464d918d363432a2e1df5f) under *3rd Party Service Providers*  |[ ]  YES |[ ]  NO |  |  |
| * Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity per **PCI DSS 12.8.5**
 |  |[ ]  YES |[ ]  NO |  |  |
| * Review four quarterly passing ASV scans
 |  |[ ]  YES |[ ]  NO |[ ]  N/A |
| * Add service provider to master list per **PCI DSS 12.8.1**
 |  |[ ]  YES |[ ]  NO |  |  |
| * Contract review by procurement
 |  |[ ]  YES |[ ]  NO |  |  |
| * Contract review by legal counsel
 |  |[ ]  YES |[ ]  NO |  |  |
| * Add [PCI Indemnification language](http://umurl.us/6e6O) to contract
 |  |[ ]  YES |[ ]  NO |[ ]  N/A |
| * Review of PCI Validated Payment Software (may not be required for all 3rd parties)
 | Is it listed on the PCI council’s website as a [PCI Validated Payment Software](https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_software)? |[ ]  YES |[ ]  NO |[ ]  N/A |
| * PA-DSS implementation guide or PIM (P2PE Instruction Manual) (may not be required for all 3rd parties)
 | Guide has been received and reviewed |[ ]  YES |[ ]  NO |[ ]  N/A |
| * Review of swipe devices (may not be required for all 3rd parties)
 | Is it listed on the PCI council’s website as an [approved PTS (Pin Transaction Security) Device?](https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php) |[ ]  YES |[ ]  NO |[ ]  N/A |
| * Dataflow Diagram
 | See [Diagram Guidance](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Diagram_Guidance.docx?d=w74dbb8cdbbb54b8ba55731a6d437e7f7)  |[ ]  YES |[ ]  NO |  |  |
| * Network Diagram
 | See [Diagram Guidance](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Diagram_Guidance.docx?d=w74dbb8cdbbb54b8ba55731a6d437e7f7) |[ ]  YES |[ ]  NO |[ ]  N/A |
| * Connectivity Diagram
 | See [Diagram Guidance](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Diagram_Guidance.docx?d=w74dbb8cdbbb54b8ba55731a6d437e7f7) |[ ]  YES |[ ]  NO |[ ]  N/A |
| * Proper due diligence per **PCI DSS 12.8.3**
 | Has all of the above been completed? |[ ]  YES |[ ]  NO |  |  |