# Appendix A – Security Questionnaire

|  |
| --- |
| MCCS Vendor Security Questionnaire   |
| Cloud Services Solution - Vendor Information | MCCS reviews the IT security of all Cloud-based services that store, process, or transmit data that MCCS considers to be Sensitive or Restricted. Please provide the documentation requested below and complete the questionnaire. N/A |
| **Requested Documentation** | **Document Titles** | **Comments** |
| **In addition to completing the questionnaire below, the following documentation should be provided to MCCS (as applicable or available and under a nondisclosure agreement - NDA - as needed in support of this security review.)**  | Cloud Security Alliance Consensus Assessments Initiative Questionnaire (if Cloud service provider)A vulnerability, penetration, or ethical hack report prepared by a third party (not by the vendor)Any documentation that describes your technical and security infrastructureData flow diagram (for college data processed by the application/service) | MCCS cannot validate and approve services or applications without supporting documentation. Please attach the requested documentation when returning the Security Questionnaire. |
|   |  |     |

|  |  |  |
| --- | --- | --- |
| Information Security | Information Security Questions | Comments and Notes |
| Management Program | Please describe your Security Management Program or attach a copy. Does your organization follow a particular security standard such as ISO-27001, ISO-22307, CoBIT, HITRUST, etc. or do you have your own? |   |
| Policy Reviews | Can you notify us when changes are made to your security policies or procedures? |   |
| User Access Policy | Please describe your employee termination procedures.  |   |
| Encryption Key Management   | Will our data be encrypted at rest? What algorithm? |   |
| Will our data be encrypted in transit, including between servers? What algorithm?  |   |
| Do you have an encryption key management system? If so, please tell us about it?  |   |
| Vulnerability / Patch Management   | Do you conduct vulnerability scans of the servers?  |   |
| Do you conduct application vulnerability scans?  |   |
| Please explain your patching policy, timeframes, and procedures.  |   |
| Antivirus / Malicious Software  | Do you have anti-malware or virus protection programs installed? Which programs?  |   |
| How often are your malware/virus protection programs updated? How regularly are complete scans scheduled?  |   |
| Incident Management   | How will you alert your clients if their data may have been breached? Do you have a documented security incident response plan? |   |
| Can you incorporate client-specific needs into your incident response plan?  |   |
| Can you outline for us what responsibilities are ours, and what are yours for an incident?  |   |
| Incident Reporting  | What method do you use for log management?  |   |
| Does your logging and monitoring method allow for isolation of an incident to specific tenants? |   |

|  |  |  |
| --- | --- | --- |
| Incident Response Legal Preparation   | How do you incorporate a “chain of custody” into your incident response plan? |   |
| Please share your procedures for forensic data collection and analysis? |   |
| Are you capable of supporting litigation holds (freeze of data from a specific point in time) for us? |   |
| Asset Returns | Please share a copy of your Privacy Policy.  |   |
| Audit Tools Access | How do you restrict, log, and monitor access to your systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.) |   |
| Source Code Access Restriction | Please describe your Source Code Analysis process.  |   |
| Security Architecture | Security Architecture Questions | Comments and Notes |
| User ID Credentials   | Please describe your identity management system and any options that are available to your clients.  |   |
| Does your system support both role-based and context-based access to the data? |   |
| Do you support two-factor authentication? If so, what options are available?  |   |
| Data Security / Integrity | Is your Data Security Architecture designed using an industry-standard? (ex. CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP CAESARS) |   |
| Application Security | Do you utilize NIST 800-64 (Security Considerations in the System Development Life Cycle) as the guideline for application development? Or, do you use another standard application security development framework?  |   |
| Do you utilize an automated source-code analysis tool to detect code security defects? |   |
| Data Integrity | Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data? |   |
| Production / Nonproduction Environments | Do you provide clients with separate environments for production and test processes? |   |

|  |  |  |
| --- | --- | --- |
| Remote User Multifactor Authentication | Is multi-factor authentication available for remote user access? |   |
| Segmentation  | Are systems and network environments logically separated?  |   |
| Are systems and network environments segmented to allow isolation of restricted data?  |   |
| Wireless Security  | What procedures are in place that require secure encryption for authentication and transmission during wireless transmission?  |   |
| Have vendor default passwords been changed?  |   |
| Shared Networks | How is access to systems with shared infrastructure restricted to only appropriate personnel?  |   |
| Equipment Identification | How does the information system identify and authenticate devices before establishing a network connection?  |   |
| Audit Logging / Intrusion Detection  | Are file integrity (host) and network intrusion detection (IDS) tools implemented? |   |
| Are audit logs protected from modification?  |   |
| Mobile Code  | How is mobile code monitored and controlled in your system? |   |
| Is all unauthorized mobile code prevented from executing? |   |