Third Party Vendor Policy

Third party entities play a key role in the support of hardware and software management, and operations for ASMSA (Arkansas School for Mathematics Sciences & The Arts). When properly authorized they can remotely view, copy, and modify data and audit logs; they correct software and operating system problems, monitor and fine tune system performance, monitor hardware performance and errors, modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by a third party will eliminate or reduce the risk of loss of revenue, liability, loss of trust and potential damage to ASMSA assets.

This policy must also require the third-party, and any of its subcontractors with whom it is authorized to share the data, to share only the minimum information necessary to securely return or destroy the personal information upon expiration of the contract, and to provide immediate notification to the campus, whenever there is a breach of sensitive data.

Purpose
The purpose of this policy is to provide a set of measures that will mitigate information security risks associated with third party access and third-party responsibilities and protection of ASMSA information. This policy also applies to all individuals who are responsible for the installation of new ASMSA assets and who allow third party access for maintenance, monitoring and troubleshooting purposes of existing Information systems.

Policy
Third party physical access to the data center will be enforced as stated in the Data Center Access policy and require the approval and authorization by an Information Services Director. Third party access to the data center facilities must sign a Confidential Information Agreement prior to accessing the ASMSA network. Third party access is temporary.
Third parties must comply with all applicable rules, policies and the ASMSA standards and agreements, including, but not limited to:

- Data Center Access
- Code of Business Conduct
- Acceptable use of Technology
- VPN Access
- Confidential Information Agreement

ASMSA will provide an Information Services point of contact for the third party. The contact will work with the third party to ensure they comply with these rules.

- Each third-party user with access to ASMSA sensitive information must be cleared to handle that information.
- All third-party personnel with access to any High Security System must adhere to all regulations and governance standards associated with that data (e.g., PCI and security requirements for cardholder data, FERPA requirements and HIPPA privacy rule for student records).
- Third party personnel must report all security incidents directly to their assigned point of contact.

- If third party vendor is involved in a security incident, it will have to be reported and documented in accordance to the Confidential Information Agreement.
- Third party personnel must follow all applicable ASMSA change management processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the corresponding department head. If access to the internal network is required, the user must abide by the VPN access policy.
- Third party credentials must be uniquely identifiable, and password management must follow ASMSA password policy. Third party's major work activities must be documented. Project milestones, deliverables, and "as build" documents must be submitted upon project completion.
- Upon termination of a contract or at the request of ASMSA, the third party will return or destroy all ASMSA information and provide written certification of that return or destruction within 24 hours.
- Upon termination of a contract or at the request of ASMSA, the third party must surrender all equipment and supplies immediately.
- Third parties are required to comply with ASMSA auditing requirements.

Enforcement

Violation of this Policy may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants. Additionally, individuals are subject to loss of ASMSA Information Resources access privileges and civil and criminal prosecution. Third Party Vendors shall be held accountable for payment for reimbursement of damages resulting from a disclosure, breach, data loss or other events that puts the ASMSA data at risk.

Exceptions to this Policy shall only be allowed if previously approved by the Information Services Directors and this approval is documented and verified by the Vice President of Information Services