Establishing and Maintaining an Information Security Program

All customer information is safeguarded. All data on the network is secured by Microsoft Active Directory and Group security is active. All Data is then protected by a Cisco ASA from external sources. All Data Access is provided by a security object or group, and has Vendor Software specific access security features as well.

The school establishes and maintains a comprehensive information security program. All information is secured by policy as well as software and hardware security measures. Data is protected from local disasters by sending a remote copy of all data to a remote backup service provider. Organization policies as to the use of data is also a form of protection. The college anticipates disasters that are unforeseen and use multiple backup copies of data in a remote location in the event of compromise. Data is also secured physically in the datacenter by a passkey that only allows physical access by authorized personnel.

Designated Coordinators. Designated Coordinators are used and are the systems administrators, along with IT departmental staff. They are expressly setup as data administrators in the security schema that is in the Microsoft suite of Active Directory security.

Risk assessment. Risk assessment is a mandate for GLBA compliance. An external vendor has been contacted to perform a risk assessment, and a remediation plan will be developed upon items that are determined to need remediation through the Risk Assessment Process. This will be an ongoing process that will be performed on an annual basis. Intrusion detection is provided by a Cisco ASA unit, and monitored by RTI, a vendor that provides technology solutions to organizations in an outsourced manner.

Safeguards testing/monitoring. Safeguards testing/monitoring will be implemented based on the risk assessment provided by an external vendor. This is a new required beginning in 2017 for all school systems. GLBA is requiring this be a part of data protection best practices.

Evaluation & Adjustment. Evaluation and adjustment are part of a new process that is being implemented. The college's IT Steering Committee will oversee any and all changes required by the risk assessment.

Overseeing service providers. The IT Director oversees all service providers for information technology projects.