Statement

All technologies, solutions, tools, designs, applications, and methods used within the architecture must adhere to all security and privacy policies, procedures, guidelines, and standards. Uniform security practices decrease the likelihood of a security breach.

Rationale

- Security is only as strong as the weakest link, so it is necessary to have security policies for all aspects of the architecture to ensure that the weakest link is a strong one. Doing so will help to maintain the integrity of both data and systems as well as data transport and transmission methods.

- Certain types of information are governed by local, state, and Federal laws. Failure to secure this information will lead to direct financial cost and potentially damage Loyola’s reputation.

Implications

- Security policies will be created, expanded and/or reviewed to cover all items within scope of this principle.

- Periodic auditing of systems will be performed to confirm compliance with industry governing bodies, local, state, and Federal laws.

- Proper controls around authorization and access to resources are necessary to mitigate risk and ensure public trust.

- Education and training at all levels of the organization is may-be required to ensure that security is addressed.

- Some authority and autonomy may be required to be moved from departments to ITS in order to align with the principle.

- Monitoring and auditing tools will be implemented and run regularly. The outcome will be evaluated by its systems owner.