Statement

Data is protected from unauthorized use and disclosure. This includes only providing access to data to those individuals who should have access to that data. This also includes properly classifying and protecting data according to Loyola data classification policies.

Rationale

• Failing to properly limit access to information will lead to information disclosure, which may violate laws and damage Loyola’s reputation.

• Applications, systems, data, and technologies will be protected from unauthorized access and manipulation. Information will be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, disclosure or transport and transmission of data.

• Data security is addressed from the beginning; it is more difficult and expensive to integrate data security after the fact.

Implications

• Information that is classified as Loyola Protected or Loyola Sensitive Data should only be shared with those individuals who require access to that information to perform their job functions.

• Policies outlining how to classify and protect data have been created and available online. Data is evaluated against the data classification policies and properly assigned.

• Data security safeguards should be put in place to restrict access to "view only," or "never see" whenever possible.

• Departments will need to have a Data Steward. The Data Steward is the person in each department who is responsible for assisting the department with complying with the Personal Information Protection Policies and who acts as the liaison between ITS and the department. Identify information owners who are responsible for other matters relating to the security of the department’s information.