1.0 Cyber Security Charter

Purpose of Charter: Georgia State University (GSU) holds significant assets in the form of information and physical property. During the course of carrying out the academic, research and fundraising mission, users collect and process many different types of information, including financial, academic, medical, human resources and other personal information. These information assets are a highly valued resource and all persons who use university information assets have a responsibility to protect this resource. Regulatory requirements, industry standards and best practices also impose obligations on the university to protect information relating to faculty, staff, students, and research subjects.

This Charter and the information security policies adopted by the university define the principles and terms of the Cyber Security Program and address the mission-critical need to secure all of these assets, including written and oral information transmitted and stored in telecommunications devices, documents, applications, systems, databases and networks.

People affected: This Charter affects all Georgia State University enterprise users, including faculty, staff, all other workers, and students.

Person(s) responsible for implementing, changing, enforcing and communicating this charter: Chief Innovation Officer (CIO)

Overview of Charter: This Charter and establishment of a Cyber Security Organization is in meeting with the requirements of Section 5: Information Security (IS) of the University System of Georgia (USG) IT Handbook.

Georgia State University has established information security policies and procedures designed to reduce business and operational risk and to protect

information assets from unauthorized disclosure, modification, or destruction. The degree of protection needed is based on the nature of the resource and its intended use. The university shall create and maintain an internal cyber security technology infrastructure, organization and program that ensures the following is maintained for information assets:

- **Confidentiality** — Ensuring that information is accessible only to authorized users
- **Integrity** — Safeguarding the accuracy and completeness of information and information-processing methods
- **Availability** — Making information assets available to authorized users when they need them

Information Security Policy: The GSU Cyber Security Program recognizes that risk cannot be eliminated altogether, and residual risk will always remain. It also recognizes it is impossible to regulate all possible situations in detail. For this reason, the program will align its best efforts with the university colleges and business units and introduce policies and standards that compliment institution policy, federal, state and local laws. The aim of the information security policies and standards is to provide adaptable guidance that helps managers, administrators and users mitigate risk, maintaining the necessary balance between risk mitigation and related costs.

The Cyber Security Program uses the Association of College and University Policy Administrators (http://www.acupa.org) (ACUPA) model for policy development, modified for the GSU environment.