Georgia State University

Cyber Security Charter

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 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.

2.0 Roles and Responsibilities

This Charter establishes the various functions within the Cyber Security Program and authorizes the persons described under each function to carry out the terms of the Information Security Policies.

- **Executive Managers** are senior University officials, including the Provost, Deans, Vice Presidents, Associate Deans, Department Chairs, Institute or Center Directors and Senior Business Officers, who are responsible for overseeing information security for their respective areas of responsibility and for ensuring compliance with all Information Security Policies. Refer to the 'Definitions-Roles' section for detailed Executive Manager responsibilities.

- **Chief Information Security Officer (CISO):** The CISO is responsible for implementing the Cyber Security Program and ensuring that appropriate security controls exist throughout GSU and that security awareness is increased. This specifically includes determining: methods of implementing and enforcing security policies; advising information and system owners on security-related issues; and ensuring that appropriate audits are conducted. The CISO and the information security team responsibilities include day-to-day management of the program.

  Only for the purposes of audits, responding to security incidents, and investigation of policy violations or criminal activity in support of legal or law enforcement, the university Executive Managers have granted authority to the Cyber Security Program office to have unrestricted access to GSU enterprise facilities, data, networks, systems, and computer hosts, to include cloud and

third-party hosting instances. Refer to the ‘Definitions-Roles’ section for detailed CISO responsibilities.

- **Information Security Steering Committee:** The Information Security Steering Committee is a multidisciplinary group that includes representatives from Internal Auditing, Risk Management, Information Technology, Center for Instructional Innovation (CII), and GSU business units and colleges, which is led by the Chief Information Security Officer (CISO). The committee is responsible for coordination, monitoring and communication of information-security-related matters throughout the university.
- **Information Security Liaison (ISL):** Each one of GSUs business units, colleges, and departments must appoint an Information Security Liaison (ISL) or coordinator who must be approved by the CISO. The security liaisons and/or coordinators are responsible for the review and communication of the security controls established by the Information Security Steering Committee. They will be the point of contact for all business unit, department, and college-specific information security activities. Refer to the ‘Definitions-Roles’ section for detailed ISL responsibilities.

  Data Owners: USG IT handbook defines Data Owners as organizations within the USG which are “responsible for all data being read, created, collected, reported, updated, or deleted by offices of the organization.

  As the Chief Executive Officer (CEO), the GSU President is the ultimate data owner of GSU data. The president may choose to delegate responsibility to Data Trustees and is responsible for the identification, appointment and accountability of the Data Trustees.

  Data Owners will inform the Data Governance and Data Management Committee of their data trustee appointments including office, name, and contact information of the incumbent. Refer to the ‘Definitions-Roles’ section for detailed Data Owner responsibilities.

- **Data Trustees:** Data Trustees, designated by the Data Owner, are executives of GSU who have overall responsibility for the data being read, created, collected, reported, updated or deleted by the units reporting to them. These positions/offices would normally be cabinet-level positions reporting directly to the entity Data Owner.” Refer to the ‘Definitions-Roles’ section for detailed Data Trustee responsibilities.
- **Data Stewards:** Data Stewards, designated by the Data Trustees, are offices/positions responsible for the data being read, used, created, collected,

reported, updated or deleted, and the technology used to do so, in their functional areas. Positions held by the Data Stewards normally would report directly to the Data Trustee. Data stewards recommend policies to the Data Trustees, and establish procedures and guidelines concerning the access to, completeness, accuracy, privacy, and integrity of the data for which they are responsible. Refer to the 'Definitions-Roles' section for detailed Data Steward responsibilities.

- **System Owners:** System Owners are individuals (or roles) with administrative responsibility for a system or other computing resource. Unlike information owners, who are responsible for the information/data only, system owners are responsible for the system hardware, the operating system, databases and applications residing on systems. System Owners may delegate actual tasks to others (for example, computer systems administrators), and both act in response to the defined needs and requirements of the information/data owner. Refer to the 'Definitions-Roles' section for detailed System Owners responsibilities.
- **Computer Security Incident Response Team (CSIRT):** The Computer Security Incident Response Team includes the CISO and the individuals responsible for computer networks and data center operations, and other organization stakeholders, as defined in the comprehensive GSU Incident Response Plan. The CSIRT defines information security emergency situations, determines when such situations exist and initiates appropriate countermeasures according to incident response plans and procedures.
- **Employees:** All GSU employees, including temporary, part-time and contract workers, and all other people authorized to perform work on GSU premises or otherwise granted access to GSU information or systems are responsible for ensuring that GSU information assets are used appropriately at all times. Specifically, they must ensure, to the best of their abilities, that information assets and systems are used only in support of the GSU's business operations, that information is not improperly disclosed, modified or endangered, and that access to GSU information resources is not made available to any unauthorized person.

3.0 References

NIST publication for an introduction to Computer Security:
NIST Pub 800-12 Introduction to Computer Security (NIST Handbook)
http://csrc.nist.gov

Georgia Technology Authority (GTA) Policy:
PS-08-005.01 Enterprise Information Security Charter
https://gta.georgia.gov/psg/article/enterprise-information-security-charter

University System of Georgia IT Handbook:
http://www.usg.edu/information_technology_handbook/

4.0 Related Enterprise Polices

Information Security Management System
https://app.gsu.edu/policies/search_policies.cfm?view_policy=5591
Information Systems Ethics
https://app.gsu.edu/policies/search_policies.cfm?view_policy=5596
University Information Systems Use
https://app.gsu.edu/policies/search_policies.cfm?view_policy=4608

5.0 Definitions - Roles

- **Executive Managers** are senior University officials, including the Provost, Deans, Vice Presidents, Department Chairs, Institute or Center Directors and Senior Business Officers, who are responsible for overseeing information security for their respective areas of responsibility and ensuring compliance with all Information Security Policies. Responsibilities include, but are not limited to:
    - Ensuring that each System Owner and Data Owner in their respective areas of responsibility appropriately identify and classify data in accordance with the GSU Data Classification Policy: 7.20.04 Data Classification, Access and Information Protection
    - Ensuring that each such System Owner and Data Owner receives training on how to handle sensitive data and confidential data; and
    - Ensuring an Information Security Liaison is assigned for his/her area of responsibility and that the liaison works collaboratively with the Cyber Security Program office in dealing with matters of information security.

- **Chief Information Security Officer (CISO):** The CISO is responsible for implementing the Cyber Security Program and ensuring that appropriate security controls exist throughout GSU and that security awareness is increased. This specifically includes determining: methods of implementing and enforcing security policies; advising information and system owners on

security-related issues; and ensuring that appropriate audits are conducted. The CISO and the information security team responsibilities include day-to-day management of the program, including:

- Developing, documenting and disseminating the information security policies, standards, and guidelines;
- Educating and training university personnel in information security matters;
- Communicating information regarding the information security policies, standards, and guidelines;
- Translating the information security policies into technical requirements, standards and procedures;
- Developing and executing the Risk Management Program;
- Collaborating with Data Owners and System Owners to determine the appropriate means of using and protecting information resources; and
- Authorizing any required exceptions to any information security policy or the USG IT Handbook and reporting such exceptions to the university executive cabinet or the USG respectively.

In addition to the responsibilities listed above, and only for the purposes of audits, responding to security incidents, and investigation of policy violations or criminal activity in support of legal or law enforcement, the university Executive Managers have granted authority to the Cyber Security Program office to have unrestricted access to GSU enterprise facilities, data, networks, systems, computer hosts, to include cloud and third-party hosting instances, to conduct the following activities:

- Monitoring communications and data that use the university network or systems for transmission or storage;
- Monitoring use of the university's information resources with Data Loss Prevention (DLP) tools, to identify sensitive or confidential information being used inappropriately;
- Conducting vulnerability scanning of any information resources connected to the University's network;
- Conducting security assessments of systems, server centers and data centers;
- Disconnecting information resources form the university network that present a security risk:
- Erasing all data stored on personal endpoints previously used for University business, as requested or required; and

- Leading and managing the University Computer-Security Incident Response Team (CSIRT), in connection with any breach or compromise of sensitive data, to the extent provided for in the USG Incident Management standard. 5.3 USG Incident Management Standard

Data Owner: The USG IT Handbook Section 9.2.2 defines the role of Data owner is as follows:

"The individual participant organization is responsible for all data being read, created, collected, reported, updated, or deleted by offices of the organization. As the chief executive officer, the president of the USG institution or the head of other USG participant organizations is identified as the data owner of the institutional data. Furthermore the Data Owner is responsible for the identification, appointment and accountability of Data trustees."

Data Trustees: The USG IT Handbook Section 9.2.3 defines the role of Data Trustees:

Data Trustees, designated by the Data Owner, are executives of GSU who have overall responsibility for the data being read, created, collected, reported, updated or deleted by the units reporting to them. These positions/offices would normally be cabinet-level positions reporting directly to the entity Data Owner."

Responsibilities of the Data Trustees include, but are not necessarily limited to:

- Ensuring that data accessed and used by units reporting to them is done so in ways consistent with the mission of the University
- The identification, appointment and accountability of Data Stewards within the functional area(s) for which they are responsible. The Data Trustees will inform the participant organization's Data Governance and Data Management Committee of their Data Steward appointments, including office, name, and contact information of the incumbent
- Participating as a member of the strategic Data Governance and Management committee
- Communicating concerns about data quality to the Data Owner.

Data Stewards: The USG IT Handbook Section 9.2.4 defines the role of Data Stewards is as:

“Data stewards, designated by the data trustees, are offices/positions responsible for the data being read, used, created, collected, reported, updated or deleted, and the technology used to do so, in their functional areas. Positions held by the data stewards normally would report directly to the data trustee. Data stewards recommend policies to the data trustees, and establish procedures and guidelines concerning the access to, completeness, accuracy, privacy, and integrity of the data for which they are responsible.”

Responsibilities of the Data Stewards include, but are not necessarily limited to:

- Ensuring data quality and data definition standards are met
- Identifying the privacy level as unrestricted, sensitive, or confidential, for functional data within their area(s) of supervision/direction
- Establishing authorization procedures with the GSU Data Governance and Data Management Committee and/or CIO to facilitate appropriate data access as defined by institutional/office data policy and ensuring security for that data
- Developing standard definitions for data elements created and/or used within the functional unit. The data definition will extend to include metadata definitions as well as the root data element definition
- Working with the GSU Data Governance and Data Management Committee, identifying and resolving issues related to stewardship of data elements, when used individually or collectively, which cross multiple units or divisions. For example, the individual data element “Social Security Number” may have more than one data steward since it is collected or used in multiple systems, such as financial, human resources, and student systems. Resolving stewardship issues for “Full-time Student” would be an example of using multiple data elements collectively to garner the informational item
- Participating as a member of the GSU Data Governance and Data Management committee(s) as appointed by the data trustee
- Communicating concerns about data quality to the data trustees

Depending on the size and compliment of the office for which the data steward is responsible, the data steward should assume or delegate steward-type roles to define the accountabilities and responsibilities that go with each data action occurring within the functional area, to wit: data definition, data collection, data reading, data creation, and so on.

Examples of these roles and associated responsibilities would likely include, but not necessarily be limited to, the following:

1. Data Definer is responsible for:
    - Defining data in the best interest of the organization;
    - Making the definition of data available to the organization; and,
    - Communicating concerns about data quality to the data steward or data trustees.
2. Data Creator is responsible for:
    - The accuracy of data being captured, created or entered;
    - The timeliness of data being captured, created or entered;
    - Defining the processes by which the technologies capture, create, or enter the data to be used; and,
    - Communicating concerns about data quality to the Data Steward or data trustees
3. Data Reader is responsible for:
    - The integrity/security of data being read/used; and,
    - Communicating concerns about data quality to the data steward or data trustees.

System Owners: System Owners are individuals (or roles) with administrative responsibility for a system or other computing resource. Unlike information owners, who are responsible for the information/data only, system owners are responsible for the system hardware, the operating system, databases and applications residing on systems. System Owners may delegate actual tasks to others (for example, computer systems administrators), and both act in response to the defined needs and requirements of the information/data owner. System Owner responsibilities include but are not limited to:

- Classifying each system in their respective areas of responsibility based on the identification and classification of data by the applicable Data Owner
- Ensuring that each such system that contains sensitive or confidential data is scheduled for risk assessment in accordance with the GSU information security risk management policy
- Establishing and implementing security requirements for each such system in consultation with the cyber security office
- Documenting and implementing audit mechanisms, timing of log reviews and log retention periods
- Maintaining an inventory of such systems
- Approving appropriate access to such systems

Information Security Liaison (ISL): Individual(s) responsible for performing as the central point of contact for a functional businesses unit, college, or

department of the institution, for matters regarding information security. The ISL's or coordinators are responsible for the review and communication of security controls established by the Information Security Steering Committee. They will be the point of contact for all business unit, department, and college-specific information security activities. With support and assistance from the GSU Cyber Security Program office, their responsibilities include:

- Performing risk management analysis to identify areas of risk and to develop security measures to prevent loss
- Developing and implementing IT system security plans, projects and initiatives
- Planning, implementing, and coordinating security measures and controls for information systems to regulate access to computer data and prevent unauthorized modification, destruction, or disclosure of information
- Plan and implement encryption system for the protection of data, data storage, and transmission paths
- Monitors use of data files and regulates access to safeguard data in computer files
- Installs, maintains, and supports information security products and services
- Works with business owners, IT managers, staff, and vendors to provide timely and efficient IT coordination of security services to meet the college or department needs
- Serve as Subject Matter Expert (SME) representing the college or department on all issues relating to area information security
- May create or contribute to reporting on status of college or department information security initiatives and projects
- Attend training and other learning opportunities to increase and maintain knowledge and skills pertinent to information security, including working to obtain industry related certifications

6.0 Definitions - Terms

Confidential Data: Any information that is contractually protected as confidential information and any other information that is considered by the University appropriate for confidential treatment. See the USG Data Classification Policy here: http://www.usg.edu/information_technology_handbook/section9/C2298

Data: All items of information that are created, used, stored or transmitted by the University community for the purpose of carrying out the institutional mission of teaching, research and clinical care and all data used in the execution of the University's required business functions.

Data Governance and Data Management Committee: A Data Governance and Management Committee is responsible for defining and managing implementation of the policies and procedures for GSU's data governance and management functions.

Specific responsibilities include, but are not necessarily limited to the following:

1. Defining data management roles and responsibilities according the USG IT Handbook standard and in other policy and procedure documentation;
2. Collating and maintaining documentation pertaining to data governance and management policy and procedure in a centralized and easy-to-access location for USG faculty and staff;
3. Identifying the Data Governance and Management Committee structure and membership; and,
4. Assisting the chairs of the functional committees to ensure effectiveness.

Email System: A server system that transmits, stores and receives emails.

Endpoint: Any desktop or laptop computer (i.e., Windows, Mac, Linux/Unix), Mobile Device or other portable device used to connect to the university wireless or wired network, access GSU email from any local or remote location or access any institutional system either owned by the university or by an individual and used for university purposes.

EPHI: Electronic Protected Health Information.

FERPA: Family Educational Rights and Privacy Act

HIPAA: Health Insurance Portability and Accountability Act and its implementing regulations as amended and supplemented by the HITECH Act and its implementing regulations, as each is amended from time to time.

HITECH: Health Information Technology for Economic and Clinical Health Act

Information Security Steering Committee: The primary vehicle for executing security governance activities such as providing a mandate for the security program, establishing and maintaining accountability, recommending security policy and participating in the approval process, mediating conflict, and allocating resources.

IP: Internet Protocol.

MAC: Media Access Control.

Mobile Device: A smart/cell phone (i.e., iPhone, Blackberry, Android, Windows phone), tablet (i.e., iPad, Nexus, Galaxy Tab and other Android based tablet) or USB/removable drive.

Network: Electronic Information Resources that are implemented to permit the transport of Data between interconnected endpoints. Network components may include routers, switches, hubs, cabling, telecommunications, VPNs and wireless access points.

Payment Card: For purposes of PCI-DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc.

PCI: Payment Card Industry.

PCI-DSS: The PCI Data Security Standard produced by the PCI–SSC, which mandates compliance requirements for enhancing the security of payment card data.

PCI-SSC: The PCI Security Standards Council, which is an open global forum of payment brands, such as American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc, that are responsible for developing the PCI-DSS.

Peer: A network participant that makes a portion of its resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by Servers or stable hosts. Examples include KaZaa, BitTorrent, Limewire and Bearshare.

Peer-to-Peer File Sharing Program: A program that allows any computer operating the program to share and make available files stored on the computer to any machine with similar software and protocol.

Removable Media: CDs, DVDs, USB flash drives, external hard drives, Zip disks, diskettes, tapes, smart cards, medical instrumentation devices and copiers.

Residual Risk: Threat that remains after all efforts to identify and eliminate risk have been made.

Risk Analysis: The process of identifying, estimating and prioritizing risks to organizational operations, assets and individuals. “Risk Assessment” is synonymous with “Risk Analysis”.

Risk Management Program: The combined processes of Risk Analysis, Risk Remediation and Risk Monitoring.

Risk Monitoring: The process of maintaining ongoing awareness of an organization’s information security risks via the risk management program.

Risk Remediation: The process of prioritizing, evaluating and implementing the appropriate risk-reducing security controls and countermeasures recommended from the risk management process. “Risk Mitigation” or “Corrective Action Planning” is synonymous with “Risk Remediation”.

RSA: The Rivest-Shamir-Adleman Internet encryption and authentication system.

Sensitive Data: Any information protected by federal, state and local laws and regulations and industry standards, such as HIPAA, HITECH, FERPA, and similar state laws and PCI-DSS. See the USG Data Classification policy here: http://www.usg.edu/information_technology_handbook/section9/C2298

Server: Any computing device that provides computing services, such as Systems and Applications, to Endpoints over a Network.

SMTP: Simple Mail Transfer Protocol, which is an internet transportation protocol designed to ensure the reliable and efficient transfer of emails and is used by Email Systems to deliver messages between email providers.

SSL: The Secure Sockets Layer security protocol that encapsulates other network protocols in an encrypted tunnel.

System: Server based software that resides on a single Server or multiple Servers and is used for University purposes. “Application” or “Information System” is synonymous with “System”.

User ID: A User Identifier.

VPN: Virtual Private Network.