



UNIVERSITY SYSTEM OF GEORGIA

USG INFORMATION TECHNOLOGY HANDBOOK

VERSION 2.9.5

8/23/2021

SENSITIVE

Abstract: USG Information Technology Handbook's purpose is to primarily set forth the essential standard components USG organizations must follow to meet statutory or regulatory requirements of the federal government, state government, Board of Regents (BOR) policy, information technology and cybersecurity best practices. Secondly, it is designed to provide new IT professionals within the USG the necessary information and tools to perform effectively. Finally, it serves as a useful reference document for seasoned professionals at USG organizations who need to remain current with changes in federal, state law and BOR policy.

Introduction

The University System of Georgia (USG) comprises public institutions of higher learning, a University System Office, Georgia Public Library System (GPLS), Shared Services Center (SSC), Georgia Archives and Georgia Film Academy; hereinafter referred to as USG organizations. These USG organizations represent the rich diversity of a state system spanning the spectrum of educational and research offerings. This manual respect the value of the diversity of USG organizations while providing guidance with regards to information technology (IT) operations within the USG.

Version Control

Date	Version	Description of Change
04/18/2016	1.0	Section 4.1 – Revised cost estimate, added a statement in IT Procurement Policies.
05/02/2016	2.0	PDF, structure and format, initial redesign referenced in a new structure and format.
05/17/2016	2.1	Section 5.12.3 – System-level password information added, added a statement about system-level passwords in bullet point number 4.
05/27/2016	2.2	Section 3.1 – Updated flow chart, updated “Recommended Process Flow Chart” added to match content.
05/27/2016	2.2	Section Introduction – updated entire section.
11/1/2016	2.3	As of Nov. 1, 2016, the department name changed to Cybersecurity.
11/3/2016	2.3	Section 5.13 – Revised Domain Name System, content in section was updated and revised.
11/3/2016	2.3	Section 5.13 – added link to the revised Domain Name System (DNS) Guidelines.
11/3/2016	2.3	Section Introduction – Georgia Film Academy added to the list of USG organizations.
11/17/2016	2.4	Section 1.3.2 – added clarification of information system owner roles and responsibilities within the framework of people, process and technology.
11/17/2016	2.4	Section 4.1 – updated spending limits for purchases more than \$1 million. Spending limits updated
05/15/2017	2.5	Section 1.2 – added the correct title to 1.2.1. Revised section for consistency in format and content. Added title.
05/15/2017	2.5	Section 1.3 – deleted a misplaced word. Revised section for consistency in format and content.
05/15/2017	2.5	Section 3.0 – added definitions from 3.1 and deleted definitions already stated in Introduction section. Revised section for consistency in format and content. Changed location of definitions.
05/15/2017	2.5	Section 3.1 – moved definitions to 3.0. Revised section for consistency in format and content. Changed location of definitions.
05/15/2017	2.5	Section 3.2 – deleted exceptions to log management standard. Revised section for consistency in format and content. Deleted exceptions.
05/15/2017	2.5	Section 3.3 – provided accurate title for ISO and deleted management of USG continuity of operations planning standard. Revised section for consistency in format and content. Added accurate titles and deleted standard.

05/15/2017	2.5	Section 5.3 – added “USG organizations” as stated in the Introduction section, changes made to the USG Incident Response and Reporting Standard and deleted Incident Categories and Reporting Timeframes table. Revised section for consistency in format and content. Deleted table.
05/15/2017	2.5	Section 5.10 – added content for clarification. Revised section for consistency in format and content.
09/07/2017	2.6	Section 5 – Added “USG organizations” as stated in the Introduction section and other minor editorial changes removing policy and standard where appropriate.
09/07/2017	2.7	Section 5 – Incorporated minor editorial changes recommended by University of North Georgia.
01/02/2019	2.8	Section 5.10 – Align with the NIST framework and FIPS. Revisions to required security reporting activities with corresponding due dates. Changed ISPR to CPR and revised components. New sub section “Remediation and Mitigation Tracker” added.
03/18/2019	2.9	Migrated to MS Word format, Export to PDF. Relocated Section 9 to the BPM. Value added Appendix: References, Glossary, Acronyms, and Index. Updated BOR policy reference from section 11 to section 10.
02/24/2020	2.9.1	Section 5.3 – Updated language, added baseline requirements and template to submit a plan for review. Incident Management.
02/24/2020	2.9.1	Section 5.9 – Updated language to align with Section 5.10. Awareness Training.
02/22/2020	2.9.1	Section 5.10 – Updated language and diagram to include biannual awareness training requirements. Required Reporting.
02/22/2020	2.9.1	Section 3.1.2 – Added section to standardize MFA deployment across the USG enterprise. Multifactor Authentication.
04/30/2020	2.9.2	Section 3.1.2 –Standardized MFA deployment heading. Strike “Section”.
04/30/2020	2.9.2	Section 3.1.2 – moved compliance information to table. Strike “Compliance Dates...” move to “Compliance” table pg. 18.
04/30/2020	2.9.2	Section 3.3.1 – editorial change, and cybersecurity framework (CSF) alignment. Strike extra space and add “All recovery planning must include lessons learned and update recovery strategies.”
04/30/2020	2.9.2	Section 3.3.1 – editorial change, and CSF alignment. Add “, or dependent” and add bullet 1 “Create, implement, maintain and test backup and recovery plan....”
04/30/2020	2.9.2	Section 3.3.1 – editorial change, and CSF alignment. Add bullet 2 “, and to provide timely communication.” And add bullet 3 “The communication controls ensure that information....”
04/30/2020	2.9.2	Section 5.1.1 – editorial change, and CSF alignment. Add “continuous”.
04/30/2020	2.9.2	Section 5.1.2 – editorial change, and CSF alignment. Add bullet 3 “expected dataflow diagrams,” and add bullet 4 “expected dataflow diagrams,”
04/30/2020	2.9.2	Section 5.1.2 – editorial change, and CSF alignment. Editorial corrections #6 and add “Principle of Least Function...”.
04/30/2020	2.9.2	Section 5.3.1 – editorial change, and CSF alignment. Add list “i. – v.” to # 5 and add “incident alert thresholds” to #6.
04/30/2020	2.9.2	Section 5.5 – editorial change, and CSF alignment. Add “continuous,” add “5.5.2 - Event data (logs) shall be collected and correlated from sources and sensors.”

04/30/2020	2.9.2	Section 5.5.2 – editorial change, and CSF alignment. Add “both internal and external to the organization” and add definition “Risk Register”.
04/30/2020	2.9.2	Section 5.5.5 – editorial change, and CSF alignment. Add “Continuously monitor...” and add “, which includes:” and list “a. – d.”.
04/30/2020	2.9.2	Section 5.10.1 – editorial change. Renumber Figure to 4/relocate reference to bottom.
04/30/2020	2.9.2	Section 5.11.7 – editorial change, and CSF alignment. Add “principle of least function...”.
04/30/2020	2.9.2	Section 5.13 – editorial change. Rebrand section title to “Domain Name System Management”.
04/30/2020	2.9.2	Section 5.14 – editorial change, and CSF alignment. Rebrand section title to “Information Protection Management.” Strike space in 1st paragraph, strike “of this manual”, and add “program’s protection processes will:”. Add “To improve the protection processes, ensure...” and add “information protection/”.
04/30/2020	2.9.2	Section 5.14.5 – editorial change, and CSF alignment. Add “or protocols” and “or protected” and strike “Information & ePrivacy”.
07/08/2020	2.9.3	Section 3.1, 3.3, and 5 – editorial changes, CSF and PF alignment. Update section to incorporate data privacy framework (PF) components.
08/07/2020	2.9.3	Section 6 – editorial change, CSF and PF alignment; Align with NIST Privacy Framework and NIST CSF Framework and provide IT Handbook portion of USG data privacy program.
08/07/2020	2.9.3	Entire Document, Performed a “harmful language” review.
09/16/2020	2.9.3	Section 5.3 – addition. Added Georgia Cybersecurity Board requirements for reporting.
12/18/2020	2.9.4	Entire Document, “Critical Systems” renamed to “Mission-Critical Systems” alignment to BPM
01/08/2021	2.9.4	Entire Document, Editorial Corrections
01/08/2021	2.9.4	Section 3, Section Control, Compliance – Updated table w dates, MFA Compliance Updates.
01/08/2021	2.9.4	Section 4.1.1 – CIO updated spending limit tiers for organizations, Spending Limits.
01/08/2021	2.9.4	Section 5.1 – Consolidated 5.1 & 5.2, updated removing 5.1.4, Consolidated organizational, roles and responsibility language into one section.
01/08/2021	2.9.4	Section 5.2 – Elevated 5.1.4 to new 5.2 AUP, Elevated AUP into stand-alone section.
07/15/2021	2.9.5	Entire Document, Updated Index.
07/23/2021	2.9.5	Section 5.3 – Updated new legislation notification requirements, add supplier management.
07/23/2021	2.9.5	Section 5.5 – Updated to include supplier management.
07/27/2021	2.9.5	Section 5.7 – Updating PII definition.
07/27/2021	2.9.5	Section 5.12 – Update password management standard.
08/23/2021	2.9.5	Section 5.14 – Removed redundant language.
08/23/2021	2.9.5	Section 5.15 – Updated email use and retirees.

08/23/2021	2.9.5	Section 7.1 – Add physical security.
08/23/2021	2.9.5	Section 10 – Shift from on-prem to cloud service.

Information, in all forms, is a strategic asset to USG organizations and the USG as a system. It is the responsibility of the Vice Chancellor and Chief Information Officer (USG CIO), under Board of Regents (BOR) Policy 10.2 to establish, “the procedures and guidelines under which the acquisition, development, planning, design, construction/renovation, management and operation of USG technology facilities and systems shall be accomplished.” Part of this responsibility is to prepare a manual of IT standards and best practices to be followed by USG organizations.

The hierarchy of USG IT policies and procedures is as follows:

1. *Board of Regents Policy Manual* is the top-level set of Board of Regents (BOR) approved policies from which all lower-level USG documents flow. Section 7.11 describes the Risk Management Policy including objectives and oversight. Compliance Policy is covered in Section 7.12 and defines applicability and implementation. Section 10, Information, Records & Publications, covers aspects of USG information technology including general policy, IT project authorization and cybersecurity.
2. The BOR *Business Procedures Manual* (BPM) has in recent years become important for IT and cybersecurity familiarization. Specifically, Section 12 describes Data Governance and Management which addresses governance, audit, cybersecurity and data privacy requirements.
3. *USG IT Handbook* (ITHB) is a standard containing IT and cybersecurity requirements and recommendations that establish acceptable IT and cybersecurity practices for USG organizations.
4. USG organization policies and processes establishes the detailed practices and tools used by USG organizations to meet the standards set forth in the *USG IT Handbook*.
5. Program or project policies and processes establish the detailed practices and tools to implement the standards set forth in the *USG IT Handbook* or USG organizations’ policies and processes.

This *USG IT Handbook* serves several purposes. Primarily, it sets forth the essential standard components USG organizations must follow to meet statutory or regulatory requirements of the federal government, state government, BOR policy and IT and cybersecurity standard practices. Secondly, it is designed to provide new IT and cybersecurity professionals within the USG the necessary information and tools to perform effectively. Finally, it serves as a useful reference document for seasoned professionals at USG organizations who need to remain current with changes in federal and state law and BOR policy.

This document provides direct links to reference information identifying the underlying source of some procedures and to provide broader understanding of the basis for others. Thus, the *USG IT Handbook*, while focusing on USG standards, also offers ready access to important policies, statutes and regulations that will aid the IT and cybersecurity professional in his or her daily performance of duties.

Governance, Compliance and Authority

The USG CIO fully supports this standard. USG Cybersecurity is responsible for managing and administering this standard for all USG organizations. Authority to create this standard originates from section 10 of the *BOR Policy Manual*.

This document is subject to periodic review and revision. The current online version supersedes all previous versions.

Scope

This standard applies to USG organizations and suppliers and affiliates under contract with the USG that accesses, stores or processes protected information.

Implementation and Applicability

A system wide or enterprise approach to IT operations and cybersecurity operations shall be adopted by USG organizations. It is expected that cybersecurity compliance will be embedded into each organization's cybersecurity plan. All compliance efforts will be focused on supporting the organization's objectives. Therefore, USG organizations' executive leaders or designee shall determine the direction and develop the organization's cybersecurity plans, standards and guidelines to:

- Identify and document applicable policies, procedures, laws and regulations;
- Establish the roles and responsibilities necessary to manage an information technology and cybersecurity program;
- Appoint skilled personnel into the identified roles;
- Communicate the importance of policies, standards and guidelines as defined in *BOR Policy Manual*, Section 10; and,
- Submit annually the Cybersecurity Program Review and required reporting as defined by *BOR Policy Manual*, Section 10.4.

Companion Documentation

USG Cybersecurity shall develop and publish companion documentation to enhance the USG *IT Handbook* or provide supporting documentation (e.g., templates, risk registers, system risk assessment tools and project tracking tools) to aid in the development of organizational plans and procedures.

Exceptions

Exceptions to any standard, procedure or guideline set forth in the USG *IT Handbook* shall be at the discretion of, and approved in writing by, the USG CIO or the USG Chief Information Security Officer (USG CISO). In each case, USG organizations or vendors must complete and submit an Exception Request Form (Access to the document is restricted to authorized users only) including the need, scope and extent of the exception, safeguards to be implemented to mitigate risks, specific timeframe, requesting organization and management approval. Contact USG Cybersecurity to obtain more information. Denials of requests for exceptions may be appealed.

Definitions

The following definitions of **Shall**, **Will**, **Must**, **May**, **May Not**, and **Should** are used throughout this USG *IT Handbook*.

1. **Shall**, **Will** and **Must** indicate a legal, regulatory, standard or policy requirement. **Shall** and **Will** are used for persons and organizations. **Must** is used for inanimate objects.
2. **May** indicates an option.
3. **May Not** indicates a prohibition.
4. **Should** indicates a recommendation that, in the absence of an alternative providing equal or better protection from risk, is an acceptable approach to achieve a requirement.

Table of Contents

Introduction	2
Version Control	2
Governance, Compliance and Authority	6
Scope	6
Implementation and Applicability	6
Companion Documentation	6
Exceptions	6
Definitions	7
Table of Contents	8
Table of Figures	12
Section 1. Information Technology (IT) Governance	13
Introduction	13
Section 1.1. Chief Information Officer Role and Responsibilities	13
Section 1.2. Governance Structure	14
1.2.1 Shared Governance Framework	14
1.2.2 Strategic Alignment	15
Section 1.3. IT Organization, Roles, Responsibilities and Processes	15
1.3.1 Organization	15
1.3.2 IT System Ownership Roles and Responsibilities	16
Section 1.4 Strategic Planning	18
1.4.1 Technology Direction Planning	18
1.4.2 Standards and Quality Practices	18
1.4.3 Development and Acquisition Standards	18
Section 1.5 Resource Management	18
Section 2. Project and Service Administration	20
Introduction	20
Section 2.1. Service Administration	20
2.1.1 Service Level Management Framework	21
2.1.2 Definition of IT Services	21
2.1.3 Service Support	21
Section 2.2. Project Administration	24
2.2.1 Initiation	25
2.2.2 Planning	26
2.2.3 Execution	26
2.2.4 Monitoring and Controlling	26
2.2.5 Closing	26
Section 2.3 Project Documentation Templates	26
2.3.1 Project Scope	27

2.3.2 Change Management Plan.....	27
2.3.3 Project Risk Management Plan	30
Section 3. Information Technology Management	32
Introduction	33
Section 3.1 Information System User Account Management.....	33
3.1.1 Information System User Account Management	33
3.1.2 Managing Multifactor Authentication	36
Section 3.2 Log Management	37
3.2.1 Purpose	37
3.2.2 Objective	37
3.2.3 Standard.....	37
Section 3.3 Continuity of Operations Planning	38
3.3.1 USG Continuity of Operations Planning Standard	38
Section 3.4 Network Services.....	41
3.4.1 Network Services Standard.....	41
Section 4. Financial and Human Resource Management	43
Introduction	43
Section 4.1. Technology Procurement Approval Process	43
4.1.1 Spending Limits.....	44
4.1.2 IT Procurement Policies	44
4.1.3 Requesting Approval.....	44
Section 4.2 Financial Management.....	45
Section 4.3 Human Resource Management	45
Section 5: Cybersecurity	46
USG Cybersecurity Charter	48
Section 5.1 USG Cybersecurity Program	50
5.1.1 Cybersecurity Program Plan Requirements.....	51
5.1.2 Information Security Officer (ISO)	51
5.1.3 USG Organizational Responsibilities	51
5.1.4 Policy and Procedure Management Requirements	53
Section 5.2 USG Appropriate Usage Standard	54
5.2.1 Requirements.....	54
5.2.2 Mobile Workforce Requirements	55
5.2.3 Enforcement	56
Section 5.3 Cybersecurity Incident Management.....	56
5.3.1 Cybersecurity Incident Response Plan Requirements	56
5.3.2 Cybersecurity Incident Reporting Requirements.....	58
5.3.3 Cybersecurity Events/Incidents Involving Personal Information.....	59

5.3.4 Cybersecurity Events/Incidents Involving Suppliers	60
Section 5.4 USG Information Asset Management and Protection	60
5.4.1 USG Information Asset Management Requirements	60
5.4.2 USG Information Asset Protection Requirements	60
Section 5.5 Risk Management.....	61
5.5.1 Risk Assessment and Analysis Requirements	61
5.5.2 Defining Risk Tolerance.....	63
5.5.3 USG Organizations Risk Management Programs.....	63
5.5.4 USG Cybersecurity Risk Management Process	64
Section 5.6 USG Information System Categorization	64
5.6.1 Purpose	65
5.6.2 Requirements.....	65
Section 5.7 USG Classification of Information	66
5.7.1 Classification Structure	66
5.7.2 Defining Personal Information.....	67
Section 5.8 Endpoint Security	68
5.8.1 Purpose	68
5.8.2 Discovery and Inventory	68
5.8.3 Anti-virus, Anti-malware, Anti-spyware Controls	68
5.8.4 Operating System (OS)/Application Patch Management	68
5.8.5 Maintenance	68
Section 5.9 Cybersecurity Awareness, Training and Education	69
5.9.1 Roles and Responsibilities.....	69
5.9.2 Cybersecurity Awareness, Training and Education Requirements	70
Section 5.10 Required Reporting	72
5.10.1 Required Reporting Activities	72
5.10.2 Remediation and Mitigation Tracker	74
Section 5.11 Minimum Security Standards for USG Networked Devices	75
5.11.1 Software Patch Updates	75
5.11.2 Anti-Virus, Anti-Spam, and Anti-Phishing Software.....	76
5.11.3 Host-Based Firewall or Host-Based Intrusion Prevention Software	76
5.11.4 Passwords	76
5.11.5 Encrypted Authentication.....	76
5.11.6 Physical Security	76
5.11.7 Unnecessary Services.....	76
5.11.8 Integrity and Segmentation	76
Section 5.12 Password Management	77
5.12.1 USG Password Authentication Standard	77
Section 5.13 Domain Name System Management	79

5.13.1 DNS Security.....	79
Section 5.14 Information Protection Management.....	80
5.14.1 Purpose	80
5.14.2 Identifying Red Flags.....	80
5.14.3 Detecting Red Flags.....	82
5.14.4 Responding to Red Flags	83
5.14.5 Protecting Personal Information	83
Section 5.15 Email Use and Protection	84
5.15.1 Purpose	84
5.15.2 Requirements.....	84
5.15.3 Retiree Email Account Management	85
Section 6 Data Privacy.....	86
Introduction	86
Section 6.1 USG Data Privacy Standard	87
6.1.1 Purpose	87
6.1.2 Standard.....	87
6.1.3 Applicability and Compliance.....	88
Section 6.2 USG Web Privacy Standard	88
6.2.1 Information Collection and Use	88
Section 6.3 Data Privacy Risks	88
6.3.1 IDENTIFY-P	89
6.3.2 GOVERN-P	90
6.3.3 CONTROL-P	90
Section 7 Facilities.....	91
Introduction	91
7.1 Physical and Environmental Security	91
Section 8 Bring Your Own Device (BYOD) Standard.....	93
Introduction	93
Section 8.1 Purpose	93
Section 8.2 Applicability.....	93
Section 8.3 Standards.....	94
8.3.1 Prior Approval	94
8.3.2 Security	94
8.3.3 USG Intellectual Property	95
8.3.4 Device and Application Support	95
Section 8.4 Standard Non-Compliance	95
Section 8.5 Employee Declaration Template.....	95
Section 9 Open for Future Use.....	95
Section 10 Learning Management System (LMS)	96

Introduction	96
10.1 Service Description.....	96
10.2 Governance and Institutional Oversight	96
10.3 Resource Model	97
10.3.1 Licensing and Hosting Costs.....	97
10.4 Change Management.....	97
10.5 Supplier Integration	97
Appendix A: References	98
Appendix B: Glossary	101
Appendix C: Acronyms (Common Abbreviations)	114
Index.....	116

Table of Figures

Figure 1: People, Process and Technology Framework	16
Figure 2: Recommended Process Flow	35
Figure 3: Multi-Factor Authentication	36
Figure 4: Required Reporting Diagram (Updated)	73
Figure 5: Risk Relationship Diagram – Cybersecurity and Privacy	87
Figure 6: Using NIST Frameworks to Manage Cybersecurity and Privacy Risks	89

Section 1. Information Technology (IT) Governance

Section Control

Table 1.1: Revision History

Date	Description of Change
05/02/2016	Initial redesign referenced in a new structure and format. PDF, structure and format
11/17/2016	Section 1.3.2 – added clarification of information system owner roles and responsibilities within the framework of people, process and technology. Clarification of information system owner
05/15/2017	Section 1.2 – added the correct title to 1.2.1. Revised section for consistency in format and content. Added title.
05/15/2017	Section 1.3 – deleted a misplaced word. Revised section for consistency in format and content.

Table 1.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date
1.1	Service Administration	July 2015	July 2015	December 2015

Introduction

Achieving strategic alignment between the Information Technology (IT) organizations and the enterprises they serve is an important goal for any organization. This alignment requires a process to assure that investments in IT projects and assets are directed toward achieving the organization's strategic vision, goals and objectives. Without alignment of purpose, intent and actions, the IT organization will not contribute purposefully to the overall mission.

Alignment is achieved through a variety of means, but three essential elements that should be formally prescribed are:

- Well-defined and understood role for the organization's Chief Information Officer (CIO).
- Well-defined and cultivated working relationships between the CIOs and the other Chief Officers (CxOs) also known as a governance structure.
- Well-defined and adopted organizational roles and responsibilities.
- Well-defined and implemented strategic planning process.
- A well-defined and recurring resource management program.

Section 1.1. Chief Information Officer Role and Responsibilities

A CIO in a higher education institution must be operationally sound and a skilled leader of staff, peers and causes. The CIO position must act as a fundamental partner with the other CxOs of the organization and must anticipate the organization's needs. Therefore, this position must be a contributing member of the leadership team; understand the organization's mission, purpose and intent; and provide a sound operating platform on which to launch new initiatives. The CIO may not be the subject matter expert on all things that the organization requires Information Technology (IT) to support, improve or launch. He

or she will not be the perfect combination of all who rely on him or her: a professor, a researcher, an accountant, a librarian, a scientist.

While the requirement for a strong leader is paramount, projects should not be led solely by the CIO. The CIO must be an advisor, a consultant and a co-leader of projects to achieve strategies but is not the sole person in the organization that should be advocating for an implementation of an IT solution. The implementation of any new IT solution must be sought to create, resolve or improve some business, academic or research function, and therefore should be led by the CxO responsible for that function.

While a well-defined and adopted working relationship between the CIO and other CxOs is paramount, the CIO must also have similar business relationships with key institution non-CxO-level management, such as human resources, legal counsel, audit and risk management, accreditation, compliance, campus police, deans, etc., as well as local authorities. For example, the CIO should be included directly in conversations and assessments of legal acts that impact IT operations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Electronic Communications Privacy Act (ECPA), the Family Education Rights and Privacy Act (FERPA) and other similar federal and state legislation.

Section 1.2. Governance Structure

Information Technology (IT) can be leveraged to advance the organization and to enable achievement of business goals. To best advance the organization's priorities, there is the need for greater accountability for decision making around the use of IT in the best interest of all stakeholders.

Effective IT governance is the prescribed relationship between the IT organization and its customers through established operational processes of communication and decision making. A governance structure should be established and function appropriately to foster partnership of business and IT leadership. Typically, an effective IT governance framework includes defining organizational structures (e.g., reporting relationships, advisory committees, etc.), processes, leadership, roles, responsibilities and other attributes to ensure that the organization's IT investments are aligned and delivered in accordance with established strategies and objectives.

Enterprise governance and IT governance should be strategically linked, leveraging technology and organizational resources to increase the competitive advantage of the enterprise.

1.2.1 Shared Governance Framework

The IT governance process should be defined, established and aligned with the overall organization governance and control environment. The framework is a shared governance model and should be founded on service management principles where all stakeholders (other CxOs) are identified and participate actively in processes that prioritize how IT resources are allocated for the organization's maximum benefit, and these stakeholders are collectively engaged in the shared responsibility of assuring that resources are aligned with needs.

Without the collective participation and interchange among the stakeholders about the priorities for the IT organization, customers relinquish control to the CIO by putting him or her in the position of making decisions on the priorities of where to assign resources. When resources are plenty and there is no competition among customers regarding what gets done first, this might not be a problem. However, when demand outpaces supply, the collective group needs to assist with the prioritization across the institution.

1.2.2 Strategic Alignment

The framework will lead to the collective understanding of how IT resources are deployed as well as the potential opportunities for their use. This information can then be used to determine the best use of these resources for the maximum institutional benefit. Priorities should be informed by not only the operational requisites, but also by organizational strategic plan and goals using a disciplined approach to portfolio, program and project management. The organization must have a methodology and set of practices to demonstrate prioritization of IT services and initiatives.

Section 1.3. IT Organization, Roles, Responsibilities and Processes

The IT organization must be defined by considering the requirements of the primary organization it serves. Its placement within the overall structure should be considered based on the scope and breadth of services it is expected to provide to the organization. The organization should have a reporting structure that incorporates IT into planning and decision making at the leadership level.

The CIO should be a regular contributing member of the executive leadership team in order to participate in relevant decision processes of the stakeholder groups in order to adequately anticipate technology resource needs, offer advice on technology enabled opportunities and respond to emergent requirements. Decisions about staffing levels, skills, functions, accountability, authority and supervision should be derived from these expectations.

1.3.1 Organization

Organizational Placement of the IT Function

The CIO should be placed in the overall organizational structure based on the scope and breadth of services the IT unit is expected to provide to the organization. In many complex organizations, a matrix reporting relationship among the most senior executive staff is not unusual. In smaller, less complex organizations, such hierarchies may not be necessary and a direct reporting relationship to the CEO is feasible. The important point is that it should not matter to whom the CIO reports, if the position is adequately incorporated into the organization's leadership team decision-making processes.

It is also important to distinguish between the role of the CIO and the most senior centralized line management function of the centralized IT function (VP, Director, etc.) Regardless of whether the IT functions are managed in a highly centralized or decentralized manner, the role of the CIO must be recognized as that of the Chief Information (technology) Officer. The responsibilities and authority of this role should span any direct reporting structures and cross over organizational boundaries to encompass all IT functions of the organization. This is so that the CIO is responsible for the organization's total IT footprint as it relates to policy, compliance, security and risk management of IT-enabled functions, regardless of any decentralized line management of departmental IT functions.

Management Structure

Decisions about the appropriate balance of a centralized vs. decentralized resource pool of staffing and budget resources is directly related to the expectations of the organization. The centralized IT organization structure must be defined by considering the requirements of the primary organization it serves.

IT Continuous Improvement Expectations

As with all administrative and educational support functions in higher education organizations, the Commission on Colleges expects units to engage in systematic planning and assessment processes to

assure institutional effectiveness (See SACS Core Requirement 3.3). Processes for planning, assessing and improving services must be documented. IT processes and services should be periodically and systematically assessed for effectiveness. Opportunities for improvement should be incorporated into the planning process and implemented over time.

1.3.2 IT System Ownership Roles and Responsibilities

Definition of Information System

Information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (FIPS 199&200; SP 800-18; SP 800-37; SP 800-53A; SP 800-60 and 44 U.S.C Section 3502.)

Selecting, implementing, and maintaining an appropriate set of security controls to adequately protect the information systems, products, or services employed by USG organizations requires strong collaboration between three primary audiences: information system owners, operation and cybersecurity managers, and information system developers. For responsible operation, it is critical each audience understands how evolving mission and business requirements, operational environment and system uses impact system operations.

Information System Ownership Roles

At the highest level, every IT application and service should have an identified information system owner. This individual should be the senior person in the organization responsible for the application or service and ensures that the application or services renders value to the organization. For most infrastructure services such as the local area network, the CIO is that information system owner. For most business and educational support systems, the CxO, vice chancellor, or executive director to whom the function reports are normally the information system owner. However, the designation is dependent upon the organizational structure.



Figure 1: People, Process and Technology Framework

Information system owners may appoint a functionally responsible designee as the primary liaison between the IT service unit and the customers served by the system or services provided by IT. For example, the VP of Enrollment Management who is the information system owner for the student information system might appoint the registrar as the day-to-day liaison between the customers of the enrollment management system and IT for support and service provisioning. Within the USO, the vice chancellor of academic affairs for example may be the designated system owner of GeorgiaBEST.

Information system owners serve as the focal point for the information systems, products, or services. In his or her capacity, the information system owner serves as both an owner and as the central point of contact between the system authorization process and subsystem owners. Examples of subsystems are application, networking, servers or workstations, owners or stewards of information stored, processed or transmitted by the system and owners of the mission and business functions supported by the system. Some organizations may refer to information system owners as program managers or business owners.

Information System Ownership Responsibilities

The information system owner is responsible for addressing the operational interests from the framework of people, process and technology. For example:

- People
 - The information system owner determines and communicates to IT the access rights and privileges to the information system for the purpose of ensuring compliance with regulatory and security requirements.
 - The information system owner ensures system users and support personnel receive requisite cybersecurity training.
- Process
 - In coordination with the Information Security Officer (ISO), the information system owner provides information and support for creating and maintaining the system security plan addressing the people, process and technology elements, and ensuring the system is deployed and operated in accordance with the agreed-upon security controls.
 - In coordination with the data owner or data steward, the information system owner is also responsible for maintaining a documented process describing access entitlements for the purpose of ensuring compliance with regulatory and cybersecurity requirements.
- Technology
 - Establish through contract, statement of work, memorandum of understanding, or service level agreement, and the technology responsibilities of IT in support of the information systems, products or services.
 - Provide liaison between the IT service unit and the customers served by the information systems, products or services provided by IT.

In support of the information system owner, ISOs are responsible for managing the repository of inventoried information systems, products or services; the information systems security plans associated with each information system identified, and any additional documentation collected in support of the information system security plans.

Attestation and Assessment – Based on guidance from the *USG IT Handbook* and the *BPM*, the information system owner informs IT and cybersecurity of the need to conduct user access and entitlement review as defined by process, ensures that the necessary resources are available for the effort, and provides the required system access, information and documentation to the ISO or audit authority. The information system owner in return shall receive the security assessment or audit results and guidance to address any discrepancies should there be any.

Section 1.4 Strategic Planning

Each USG organization should have an IT strategic plan that is integrated with the organization's strategic plan. The effective management of information technology services should include a strategic planning component to direct IT resources across the organization in line with the business strategy and priorities. This direction should be inclusive of all IT resources, regardless of the departmental structure. Within the planning effort, the CIO and other CxOs of the organization assume shared responsibility for ensuring that IT resources are expended toward a catalog of services and projects that provide the maximum benefit to the organization. Strategic planning efforts and discussions also improve key stakeholders' understanding of IT opportunities and limitations, provide opportunities to assess current performance, identify resource requirements and clarify the level of investment required.

IT strategic planning should be a documented process, which is considered in business goal setting and results in discernible business value through investments in IT. Risk and value-added considerations should be periodically updated in the IT strategic planning process. Realistic long-range IT plans should be developed and regularly updated to reflect changing technology and business developments. Benchmarking against well-understood and reliable industry norms should take place and be integrated with the strategy formulation process. The strategic plan should include how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organization.

1.4.1 Technology Direction Planning

Existing and emerging technologies should be analyzed to determine which technological direction is appropriate for IT strategy and business systems architecture. The planning should include identification of which technologies have the potential to create business opportunities and should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.

1.4.2 Standards and Quality Practices

Standards, procedures and practices for key IT processes should be identified and maintained. Industry best practices should be used for reference when improving and tailoring the organization's quality practices.

1.4.3 Development and Acquisition Standards

Standards for all development and acquisition that follow the life cycle of the ultimate deliverable should be adopted and maintained. This should include sign-off by the CIO and Executive Sponsor, or their designees, at key milestones based on agreed-upon criteria.

Section 1.5 Resource Management

The CIO must establish a process to periodically review current performance and capacity of IT resources, as well as forecast future needs based on workload, storage and contingency requirements. This process should highlight the adequacy, or lack, of the resources needed to support the organization.

As a goal, performance and capacity plans should be fully synchronized with the business demand forecasts; for example, enrollment growth or a significant change in business process that results in the peak demand for a resource. The IT infrastructure and business demand should be subject to regular reviews to ensure that optimum capacity is achieved at the lowest possible cost.

Trend analysis should be performed to show imminent performance problems caused by increased business volumes to enable planning and avoid unexpected issues. The CIO should adjust the planning for performance and capacity following analysis of these measures.

Section 2. Project and Service Administration

Section Control

Table 2.1: Revision History

Date	Description of Change
05/02/2016	Initial redesign referenced in a new structure and format. PDF, structure and format.

Table 2.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date

Introduction

IT service can be defined as a set of related functions provided by IT systems, products or services in support of one or more business areas, which in turn may be made up of software, hardware and communications facilities perceived by the customer as a coherent and self-contained entity. An IT service may range from access to a single application, such as a general ledger system, to a complex set of facilities including many applications, as well as office automation that might be spread across several hardware and software platforms. Effective communication between IT management and their customers regarding services required is enabled by a documented definition of, and agreement on, IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on service level accomplishments. This process enables alignment between IT services and the related business requirements.

A project, by definition, is a temporary activity with a starting date, specific goals and conditions, defined responsibilities, a budget, a plan, a fixed end date and multiple parties involved. Clear and accurate definition of a project is one of the most important actions you can take to ensure the project's success. The clearer the target the more likely you are to hit it. Defining a project is a process of selection and reduction of the ideas and perspectives of those involved into a set of clearly defined objectives, key success criteria and evaluated risks. A project management framework will help maintain the organization's portfolio of projects that support its IT-enabled programs by identifying, defining, evaluating, prioritizing, selecting, initiating, managing and controlling these projects in order to ensure that the projects support the organization's objectives. The framework will help coordinate the activities and interdependencies of multiple projects, manage the contribution of all the projects within the organization to expected outcomes and resolve resource requirements and conflicts.

A documented definition of, and agreement on, required IT services and service levels must be established between IT management and organization customers. A framework for the management of all IT projects must be established to ensure the correct prioritization and coordination of all projects.

Section 2.1. Service Administration

A documented definition of, and agreement on, required IT services and service levels must be established between IT management and organization customers. This process should include monitoring and timely reporting to stakeholders on service level accomplishments. Portfolio

management includes the demand and resource allocation across all services, programs and projects; including those resources to support internal services and projects. Programs and projects exist either to create a new service; to expand, enhance or improve (e.g., to reduce risk or cost per planning unit or to add features); or to retire a service. Service levels must be periodically re-evaluated to ensure alignment of IT and business objectives. All service level management processes should be subject to continuous improvement. Customer satisfaction levels should be regularly monitored and managed. Expected service levels must reflect strategic goals of the organization and be evaluated against industry norms. IT management must have the resources and accountability afforded by the institution to meet service level targets. Senior management should monitor performance metrics as part of a continuous improvement process.

2.1.1 Service Level Management Framework

A framework that provides a formalized service level management process between customers and the service provider must be defined. This framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding. The framework should also define the organizational structure for service level management; covering the roles, tasks and responsibilities of internal and external service providers and customers. The framework should include processes for creating service requirements, service definitions and funding sources, as well as documentation such as Service Level Agreements (SLAs) and Operating Level Agreements (OLAs). Specified service level performance criteria should be continuously monitored and reports on the achievements of service levels should be provided in a format that is meaningful to stakeholders. The monitoring statistics should be analyzed and acted upon to identify positive and negative trends for individual and overall services provided. SLAs and their associated contracts, if applicable, with internal and external service providers should be regularly reviewed to ensure that they are effective, up-to-date and that changes in requirements have been considered.

2.1.2 Definition of IT Services

Definitions of IT services should be based on service characteristics and business requirements. These definitions should be organized and stored centrally.

2.1.3 Service Support

Service Support must focus on the IT end user, ensuring that they have access to the appropriate IT services to perform their business functions. Effective service support management requires the identification and classification, root cause analysis and resolution of issues. This process also includes the formulation of recommendations for improvement, maintenance of issue records and review of the status of corrective actions. This process should include setting up a service desk or service request function with registration, issue escalation, trend and root cause analysis and resolution. In addition, root causes of issues, such as poor user training, can be identified and addressed through effective reporting.

Service Desk/Service Request Function

A service desk or service request function, which is the end user interface with IT, should be established to register, communicate, analyze and route all customer service requests, reported issues and information requests. It should be the single point-of-contact for all end user issues. Its first function should be to create a ticket in an issue tracking system that will allow logging and tracking of service support requests. Issues must be classified according to type, business, and service priority. There must be monitoring, and escalation procedures based on agreed-upon service levels relative to the

appropriate SLA that allow classification and prioritization of any service support requests (e.g., an incident, problem, service request, information request, etc.).

Once an issue has been logged, an attempt should be made to solve the issue at this level. If the issue cannot be resolved at this level, then it should be passed to a second or third level within the issue tracking system and routed to the appropriate personnel for analysis and resolution. The service desk or service request function should work closely with related processes such as change management, release management and configuration management. Customers must be kept informed of the status of their requests. The function must also include a way to measure the end user's satisfaction with the quality of the service support and IT services. As a goal, the service desk and service request function should be established and well organized and take on a customer service orientation by being knowledgeable, customer-focused and helpful. Advice should be consistent, and incidents resolved quickly within a structured escalation process. Extensive, comprehensive FAQs should be an integral part of the knowledge base, with tools in place to enable a user to self-diagnose and resolve issues. Metrics must be systematically measured and reported. Management should use an integrated tool for performance statistics of the service desk and service request function. Processes should be refined to the level of best industry practices, based on the results of analyzing performance indicators, continuous improvement and benchmarking with other organizations.

Clarification of Issues

Processes to classify issues that have been identified and reported by end users must be implemented to determine category, impact, urgency and priority. Issues should be identified as incidents or problems, and be categorized into related groups, such as hardware, software, etc., as appropriate. These groups may match the organizational responsibilities of the end user and customer base and should be the basis for allocating problems to the IT support staff. Note that incident management differs from problem management. The purpose of incident management is to return the service to normal level as soon as possible with the smallest possible business impact. The principal purpose of problem management is to find and resolve the root cause of a problem and prevent further incidents.

Incident Management

An incident is any event that is not part of the standard operation of the service and causes, or may cause, an interruption or a reduction of the quality of the service. Incident Management aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations. Normal service operation is defined here as service operation within SLA limits.

Problem Management

A problem is a condition often identified because of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown. Problem Management aims to resolve the root causes of incidents to minimize the adverse impact of incidents and problems and to prevent recurrence of incidents. The objective of problem management is to reduce the number and severity of incidents and report findings in documentation that is available for the first line and second line of the service desk and service request function.

Tracking of Issues

The issue management process must provide for adequate audit trail capabilities that allow for tracking, analyzing and determining the root cause of all reported issues considering:

- All outstanding issues.

- All associated configuration items.
- Known and suspected issues and errors.
- Tracking of issue trends.

The process should be able to identify and initiate sustainable solutions to reported issues that address the root cause, raising change requests via the established change management process. Throughout the resolution process, regular reports should be made on the progress of resolving reported issues. The continuing impact of reported issues on end user services and against established SLAs should also be monitored.

If this impact becomes severe or reaches established SLA thresholds, the issue management process must escalate the problem.

Escalation of Issues

Service desk and service request function procedures must be established so that issues that cannot be resolved immediately are appropriately escalated according to the guidelines established in the SLAs. Workarounds should be provided if appropriate. These procedures should ensure that issue ownership and life cycle monitoring remain with the service desk for all user issues, regardless of which IT group is working on the resolutions.

Resolution and Closure of Issues

Procedures must be put in place to close issues either after confirmation of successful resolution of the issue or after agreement on how to alternatively handle the issue. When an issue has been resolved, these procedures should ensure that the service desk records the resolution steps and confirms that the customer agrees with the action taken. Unresolved issues should be recorded and reported to provide information for the timely monitoring and clearance of such issues.

Reporting and Analysis

The issue management system must be able to produce reports of service desk activity so that management can measure service performance and service response times, as well as identify trends or recurring issues so that service can be continually improved.

Assessment

An effective service support process requires well-defined monitoring procedures, including self-assessments and third-party reviews. These procedures should allow continuous monitoring and benchmarking to improve the customer service environment and framework. Remedial actions arising from these assessments and reviews should be identified, initiated, implemented and tracked.

Service Metrics

The need for metrics is driven by the desire to deliver and demonstrate high-quality service. The type of metrics collected is driven by the business and IT requirements for service reporting and Key Performance Indicators (KPIs). Ultimately, metrics collection and aggregation provide input into key business decisions such as how to equitably allocate costs. Service metrics represent the KPIs of an IT service. They should be based on measurable attributes of the associated process, network, system, application, server or storage components that support the service. For example, the availability of a service may be dependent on the combined availability of various underlying components as well as a minimum volume of transactions processed by an application.

The basic requirement of any collected metric is that it be derived from performance and availability attributes of the specified target. Extended metrics will rely on more sophisticated attributes related to

resource usage, transactions and process efficiency. Other metrics specify indicators that are more representative of business processes and operations. The technical infrastructure required to measure and collect metric data varies widely depending on the characteristics of the metrics and the availability of supporting data. There are dependencies on how the measured resource is instrumented and how the information can be collected. The complexity, effort and cost-of-collection required to maintain such an infrastructure in a dynamic environment is another important element. Use of standards, best practices and effective integration are important considerations for successful and maintainable IT service metering. To reduce the overhead associated with common data collection implementations that use proprietary agents, IT service metrics should be based on agents with mechanisms supplied by applications and operating systems vendors or with agents based on standards. This nonproprietary approach helps minimize support overhead as well as speed deployment as it reduces much of the upfront planning and configuration efforts.

Service Benchmarking

IT service benchmarking defines a strategic management method that compares the performance of one IT service provider with the IT services of other institutions or organizations. Performance means both efficiency and effectiveness criteria. The comparison can be carried out within one organization, but also on an enterprise basis. The objective of IT benchmarking is to identify optimization potentials and extrapolate recommendations on how performance could be improved. The benchmark is the so-called best practice. This means that the organization or its processes provided by the IT service in question largely meets the defined efficiency and effectiveness criteria of the best.

A typical benchmarking procedure may include, but is not limited to:

- Identifying efficiency and effectiveness criteria that serve as comparative factors and asking how IT services within an operative process should be changing.
- Finding internal and external benchmarking partners or donors to set up a comparative platform, with each partner being prepared to share the necessary information.
- Setting up a key data system by taking the comparability into account, with a clear and definition-based boundary to ensure a fair comparative platform.
- Analyzing the database and identifying the best-practice participants and defining the target benchmark.
- Identifying optimization potentials and guidelines by comparison with the best practice.
- Calculating theoretical savings potentials.
- Extrapolating objectives to close the gap to best practice.
- Setting up an implementation plan.
- Controlling results and improvements.

Section 2.2. Project Administration

A framework for the management of all IT projects must be established to ensure the correct prioritization and coordination according to priorities established by the Board of Regents, the Chancellor, institution presidents and organization directors. This framework may include, but is not limited to:

1. Business case.

2. Project scope to include deliverables and requirements.
3. Sponsor engagement and appropriate sign-off.
4. Schedule, preferably including resources.
5. Method for tracking issues, risks and decisions.
6. Change management approach.
7. Risk management approach.
8. Testing and implementation.
9. Post-implementation review.

The project management framework should define the scope and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken. This approach:

1. Insures project risk management and value-added delivery to the organization.
2. Reduces the risk of unexpected costs and project cancellation.
3. Improves communications to, and involvement of, stakeholders and end users.
4. Ensures the value and quality of project deliverables.
5. Maximizes their contribution to IT-enabled programs.

A proven, full life cycle project administration methodology¹ must be implemented, enforced and integrated into the culture of the entire organization. An ongoing initiative to identify and institutionalize best project management practices should be implemented. An IT strategy for sourcing development and operational projects should also be defined and implemented.

2.2.1 Initiation

A project management approach should be established corresponding with the size, complexity and regulatory requirements of each project. The project governance structure should include the roles, responsibilities and accountabilities of the various personnel involved in the project and the mechanisms through which they can meet those responsibilities. These personnel may include, but are not limited to:

1. Program or executive sponsors
2. Project sponsors
3. Project leads
4. IT steering committee
5. Project manager
6. Project management organization
7. Stakeholders
8. End users

All IT projects must have sponsors with sufficient authority to own the execution of the project within the overall organization strategic plan. These sponsors should exist outside of the IT department. Stakeholders and end users should be engaged in the work of the program, including projects, to ensure success and collaboration. The project manager and project management organization should work with the appropriate personnel to develop the appropriate documentation for the project during initiation. This documentation may include several types of documents, such as a business case, a project scope

¹ Reference: Institute, P.M. (2008). A guide to the project management body of knowledge. (4th Ed.). Newton Square: Project Management Inst.

and other documents that define key aspects of the project such as goals, benefits, risks, resources required, sponsor, success criteria and metrics, etc. Templates for a business case, project scope, change management plan and risk management plan are shown in Section 2.3.

2.2.2 Planning

A formal, approved integrated project plan should be established to guide project execution throughout the life of the project. Changes to this plan should be approved in line with the IT governance framework. Planning should include documentation of program and project interdependencies to minimize risk to all projects undertaken within a program or service. The organization and project team should develop the project plan, including the project schedule, change management and communications plans, and the way in which risks, decisions and issues will be tracked and managed during the project life cycle. The change management plan should establish the mechanism by which all changes to the project baseline, including cost, schedule, scope and quality will be appropriately reviewed, approved and incorporated. Project risks should be eliminated or minimized through a systematic process of planning, identifying, analyzing, monitoring, controlling and responding to the areas or events that have the potential to cause unwanted change. Risks should be identified and centrally recorded.

2.2.3 Execution

During the execution phase, the project team should execute the project plan in compliance with the project scope. Approval of the project should be based on IT governance decisions. Approval of subsequent phases should be based on review and acceptance of the deliverables from the previous phase. In the event of overlapping project phases, an approval point should be established by program and project sponsors to authorize project progression.

2.2.4 Monitoring and Controlling

The project timeline, scope and budget must be monitored and controlled per the project and change management plans during the controlling phase of the project. Project performance should be measured against key project performance scope, schedule, quality, cost and risk criteria. Deviations from the project plan should be identified and assessed for impact on the project. Results should be reported to key stakeholders. Remedial action should be recommended, implemented and monitored in-line with the program and project governance framework.

2.2.5 Closing

A project should be closed when the project sponsor agrees that the project scope has been satisfied. At the end of each project, the project stakeholders must ascertain whether the project has delivered the planned results and benefits. Any outstanding action items that are required to achieve the planned results of the project should be identified, communicated and disposed of as needed. Project documentation should be archived, and lessons learned for use on future programs and projects should be identified and documented.

Section 2.3 Project Documentation Templates

The following templates are provided as examples that could be used as a starting point for developing project documentation. Templates already in place at your institution are acceptable as well.

2.3.1 Project Scope

The project scope document must include project goals and deliverables.

Table 2.3: Project Goals and Deliverables

Project Name		Date	
Project Sponsor		IT Project Sponsor	
Program Manager		Project Manager	
Executive Summary	High level description of the project, linkages to strategic goals, and justification.		
Project Description	Define who, what, when and why of the project.		
Project Goals and Objectives	These may come from the business case but should be refined if additional information is available.		
Project Scope	Specific features, functions, and regulations that must be complied with for the project to be deemed a success. Specify those features and functions that are out of scope for this project.		
Project Deliverables	What will be produced because of this project?		
Assumptions and Constraints/Boundaries	Assumptions are conditions that are assumed to be true or to exist and will impact the success of the project. Constraints and boundaries are limits to the project deliverables and sphere of influence.		
Project Dependencies	Conditions that must exist or be met for the project to move forward and successfully meet its objectives.		

Signature

Project Sponsor

Date

2.3.2 Change Management Plan

Purpose

The purpose of a Change Management Plan is to set out the methods and procedures to handle all changes affecting this project's:

- Resources, costs, and timing as set out in the project plan.
- Deliverable, product and process quality.

A change management plan exists to provide a formal process for:

- Submission and receipt of change requests.
- Review and logging of change requests.
- Determination of the feasibility of change requests.
- Approval of change requests.
- Implementation and closure of change requests.

All project changes should enter the Change Management cycle in the format of a Change Request.

Legitimate changes to the product/project may stem from:

- Responses to problems internal to the project.
- Externally imposed requirements.
- Change in business requirements or strategy.
- Proactive changes to improve performance or benefit.

A Change Management Plan should employ an industry standard cyclical approach to:

- Ensure standardized methods, processes and procedures are used for all project changes;
- Facilitate efficient and prompt handling of all changes; and,

- Maintain a proper balance between the benefits of change and the detrimental impact of change on the Project Plan.

Table 2.4: Change Management Roles and Responsibilities

Role	Responsibilities
Project manager	<ul style="list-style-type: none"> • Develop change management plan • Take change requests to change review board • Monitor change requests • Log change requests
Project team	<ul style="list-style-type: none"> • Evaluate change requests and estimate impact to scope, schedule, and budget
Change Review Board	<ul style="list-style-type: none"> • Evaluate change requests, make decisions as to whether they are accepted, rejected, or deferred
Sponsors (Project/IT)	<ul style="list-style-type: none"> • Approve change management plan

Table 2.5: Change Review Board

Role	Name
Project manager	
Change Review Board leader	
Technical Review Board members	
Change Review Board members	

Table 2.6: Change Control Documents

Document	Function
Change request	<ul style="list-style-type: none"> • Documents desired changes as requested or discovered • Documents what the change is • Documents the rationale and benefit of the change • Documents the risk of not changing
Change/Decision log	<ul style="list-style-type: none"> • Summarizes change requests received • Track's status of change requests submitted • Documents change decisions made, when, and by whom
Type of Change	Control Document
Scope	<ul style="list-style-type: none"> • Scope statement • WBS (work breakdown structure) • Product requirements • Scope management plan
Time	<ul style="list-style-type: none"> • Schedule baseline • Schedule • Milestones • Schedule management plan
Costs	<ul style="list-style-type: none"> • Cost baseline • Budget • Cost management plan
Risk	<ul style="list-style-type: none"> • Risk management matrix • Risk management plan
Communications	<ul style="list-style-type: none"> • Communication plan • Stakeholder analysis
Resources	<ul style="list-style-type: none"> • Roles and responsibilities • Resources/staffing allocations

Change Management Procedures

A Change Management Cycle may be comprised of the following events:

- Raise and record Change Request (CR)
- Assess impact and value of change
- Present assessment results and obtain approval
- Implement change and re-baseline plan
- Close CR

Raise and Record Change Request

The change initiator prepares a Change Request and communicates the details of the change to the Project Manager. The change initiator should complete and store the Request Section. Information below reflects information typically requested on a change request form.

Request Section

Completed and sent to the project manager:

Table 2.7:

Requester Name:	
Requester Contact Information:	
Change Request Date:	
Priority:	
Summary of Change:	
Description of Change:	
Rational for Change:	
Benefit of Change:	
Date Required for Approval	

Evaluation Section

Completed and sent to the project manager and project sponsors:

Table 2.8:

Change Request ID:	
Change Request Assigned Date:	
Implication for Project:	
Risk:	
Resource Impact Statement:	
Estimated Impact on Effort:	
Estimated Impact on Cost:	
Estimated Impact on Schedule:	
Decision:	
Decision Detail:	
Decision Maker:	
Decision Date:	

Details of each change request should be recorded in the Change Log.

Assess Impact and Value of Change

The Change Request is escalated to the project core team for technical evaluation. All change requests will be reviewed at team meetings or on an as needed basis. The CR is assessed for its impact on the project plan (resources, costs and schedule) by the Project Manager and the project core team. A brief Business Case is completed with the assistance of the project core team. Present Assessment Results and Obtain Approval. The results of the CR assessment are presented to the Change Control Review Board – Steering Committee, project sponsor, or other authority. Based on the value judgment passed on the CR, it is accepted or rejected. If accepted, sign-off represents a new agreement on the updated Project Plan. The new timeline, scope, costs and schedule should be baselined.

Implement Change and Re-baseline Plan

Work should not begin on the CR until an approval has been given. At that time, the new work required by the change is undertaken and completed according to the new Project Plan.

Close Change Request

Following successful implementation and testing of the CR work, a closing entry is made in the Change Management Log.

Project Archives

This section defines where change management documentation will be stored and archived.

Signatures

The Project Sponsor signs off on the change management plan, giving authority to the team members to record, assess, track and approve or reject change requests.

2.3.3 Project Risk Management Plan

A Project Risk Management Plan is a controlling document that incorporates the goals, strategies and methods for performing risk management on a project. The Project Risk Management Plan describes all aspects of the risk identification, impact analysis and control processes. The purpose of developing such a plan is to determine the approach for performing risk management on the project.

Table 2.9: Roles and Responsibilities

Role	Responsibilities
Project Manager	<ul style="list-style-type: none">Leads the development of a Project Risk Management PlanLeads the project team through identification of risksFacilitates risk analysis with Risk Management TeamMonitors and escalates risks to the Risk Management Lead
Project Sponsor	<ul style="list-style-type: none">Approves the Risk Management Plan
Risk Management Lead	<ul style="list-style-type: none">Chairs the Risk Management TeamApproves Risk ScoringApproves risk disposition strategy
Risk Management Team	<ul style="list-style-type: none">Identifies risksConducts risk impact analysisDevelops disposition strategy recommendations
Project Team	<ul style="list-style-type: none">Identifies risks

Risk Identification, Qualification and Quantification

Methods to be used to identify risks for a project may include, but are not limited to, brainstorming sessions, historical review of similar projects and expert interviews. Risks may be identified during daily project activities, in risk assessment meetings or in critical issues sessions. Identified risks should be added to a project risk register. To determine the severity of the risks identified by the team, a probability and impact factor may be assigned to each risk. This process allows the risk management team to prioritize risks based upon the effect they may have on the project. In this template, the project manager utilizes a probability-impact matrix to give each risk a score. The chart below defines the criteria used to calculate the Risk Score. There is an assigned numeric value to each risk factor choice. The risk factor values are multiplied together to calculate the Risk Score.

Table 2.10: Risk Score

Probability	Impact	Timeline
75% - 100%	Critical: Project stops or fails	
51% - 74%	Elevated: Major impact to project timeline, costs, or scope	
26% - 50%	Moderate: May have impact to project timeline, costs, or scope	
0% - 25%	Minor: No impact to project timeline, costs, or scope	

Risk Prioritization

Once the risks are assigned a Risk Score, they may be prioritized with the highest Risk Score being given the highest priority.

Risk Response Planning

The risks for a project may be managed and controlled within the constraints of time, scope, and cost. All identified risks may be evaluated to determine how they affect the triple constraint. The project manager, with the assistance of the Risk Management team, may determine the best way to respond to each risk to ensure compliance with these constraints. The project manager may lead the Risk Management Team to assign a Risk Disposition for each identified risk. Risk Disposition options include:

- **Mitigate** – Action will be taken to manage the risk to minimize the likelihood that it will become a project issue.
- **Transfer** – The risk will be managed outside of the project. The transfer recipient must be identified and accept transfer.
- **Accept** – Risk Management Lead approves no action will be taken for this risk.

Risk Monitoring and Control

It is recommended that risks are monitored during the time the project is exposed to each risk. Risk monitoring must be a continuous process throughout the life of a project. As risk mitigation tasks approach on the project schedule, the project manager should provide the necessary status updates that include the risk status, identification of trigger conditions, and the documentation of the results of the risk response.

Risk Register

The Risk Register is a log of all identified risks, their probability and impact to the project, the category they belong to, mitigation strategy and when the risk will occur. An example of a Project Risk Register is shown below.

Table 2.11: Risk Register

ID	Description	Timeline	Probability	Impact	Score	Risk Exposure	Risk Status	Disposition	Trigger Date	Action Description	Owner	Updated Date
1.												
2.												
3.												

See Risk Identification, above, for recommended approaches to identify risks to be entered into the Risk Register. Based on the identified risks and timeframes in the risk register, each risk may be added to the project plan. At the appropriate time in the plan, prior to when the risk is most likely to occur, the project manager may assign a risk manager to ensure adherence to the agreed upon mitigation strategy. The Risk Register should be maintained in a central location available to the entire project team.

Signature

The Project Sponsor must sign the risk plan, thereby agreeing to the project approach for managing project risks.

Section 3. Information Technology Management

Section Control

Table 3.1: Revision History

Date	Description of Change
05/02/2016	Initial redesign referenced in a new structure and format. PDF, structure and format
05/27/2016	Section 3.1 – updated “Recommended Process Flow Chart” added to match content. Updated flow chart
05/15/2017	Section 3.0 – added definitions from 3.1 and deleted definitions already stated in Introduction section. Section 3.1 – moved definitions to 3.0. Revised section for consistency in format and content. Changed location of definitions.
05/15/2017	Section 3.2 – deleted exceptions to log management standard. Revised section for consistency in format and content. Deleted exceptions.
05/15/2017	Section 3.3 – provided accurate title for ISO and deleted management of USG continuity of operations planning standard. Revised section for consistency in format and content. Added accurate titles and deleted standard.
02/22/2020	Section 3.1.2 – Added section to standardize MFA deployment across the USG enterprise. Managing Multifactor Authentication
04/30/2020	Section 3.1.2 –Standardized MFA deployment heading. Strike “Section”
04/30/2020	Section 3.1.2 – moved compliance information to table. Strike “Compliance Dates...” move to “Compliance” table pg. 18
04/30/2020	Section 3.3.1 – editorial change, and CSF alignment. Strike extra space and add “All recovery planning must include lessons learned and update recovery strategies.”
04/30/2020	Section 3.3.1 – editorial change, and CSF alignment. Add “, or dependent” and add bullet 1 “Create, implement, maintain and test backup and recovery plan....”
04/30/2020	Section 3.3.1 – editorial change, and CSF alignment. Add bullet 2 “, and to provide timely communication.” And add bullet 3 “The communication controls ensure that information....”
07/09/2020	Section 3.1 – editorial change, and CSF alignment. Strike “Introduction”
07/09/2020	Section 3.1.1 – editorial change, and CSF alignment. Edit and add content “provisioned” and “deprovisioned”
07/09/2020	Section 3.1.1.1 – editorial change, and CSF alignment. Add content, “to address both cybersecurity and privacy concerns.”
07/09/2020	Section 3.2.1 – editorial change, and CSF alignment. Add sentence to second paragraph.
07/09/2020	Section 3.2.2 – editorial change, and CSF alignment. Add bullet and content, “Define criteria...” and “or “mission-critical systems”
07/09/2020	Section 3.2.3 – editorial change, and CSF alignment. Add content to final paragraph.
01/08/2021	Section 3, Section Control, Compliance – Updated table with dates. MFA Compliance Update

TBD	Section 3.3 – complete restructuring and CSF and PF alignment. Update content to align with the larger enterprise Continuity of Operations Project focusing on IT and Cybersecurity incident response, disaster recovery and contingency planning.
-----	--

Table 3.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date
3.1	Information System User Account Management	November 2012	March 2013	July 2013
3.1.2	Implementation plans must be submitted	January 2018	February 2020	December 2019
3.1.2	Implementation must be complete	June 2019	February 2020	December 2019
3.1.2	Multifactor Authentication (MFA) – OneUSG (Tier I)	October 2019	March 2020	December 2019
3.1.2	MFA - Systems storing or processing critical or protected information. Examples include databases, data warehouses, email, internet facing servers and portals (Tier II).	October 2019	March 2020	December 2021
3.1.2	MFA - Systems permitting privileged access, remote access, server(s) critical to supporting business functions and single sign-on systems (Tier III).	October 2019	March 2020	December 2022

Introduction

Knowledge Management provides IT systems, tools, governance and support to facilitate the creation and management of data and the use of information and knowledge for effective analysis and decision making. IT Management establishes and advances an environment and a set of practices that support agile and accessible collection, transformation, warehousing, retrieval, analysis and exchange of vital enterprise data and decision-support information.

Section 3.1 Information System User Account Management

IT Management establishes practices that support agile and accessible collection, transformation, warehousing, retrieval, analysis and exchange of vital enterprise data and decision-support information. Knowledge Management provides information technology systems, tools, governance and support to create and manage data as well as the use of information and knowledge for effective analysis and decision-making.

3.1.1 Information System User Account Management

Controlling access to information systems, products or services and managing user accounts are critical business processes that support effective use of information resources. Effective use of information resources is a shared responsibility among human resource management (HRM), system owners and data stewards. Examples of these key responsibilities can be found with the student information system where the registrar may serve as the data steward in defining access procedures and guidelines for at least part of the system, while IT may serve as the system owner by developing, integrating and

maintaining interfaces to the system, while HRM ensures that personnel changes affecting user access to the system are communicated to concerned parties.

At its core, this section refers to the process by which an individual's access and permissions is activated (provisioned), reviewed and deactivated (deprovisioned) consistent with their roles and responsibilities as an employee. To be effective, an account provisioning process should ensure that the creation of accounts and the access to applications and data are consistent while maintaining required privacy and protecting information systems. Information systems user account management must be addressed to lower the risks and threats facing users, hosts, networks and business operations.

3.1.1.1 Information System User Account Management Procedures

The USG recognizes its information resources are strategic and vital assets belonging to the people of Georgia. These assets require a degree of protection commensurate to their value. Information systems, products or services must be protected from unauthorized access, loss, contamination or destruction. Proper management and protection are characterized by ensuring the confidentiality, integrity and availability of the system. User account access is a continual process and vital to proper management and security of information systems. HRM, system owners and data stewards will work together to create organizational procedures focused on good communication, accuracy of user account data and protection of confidential or sensitive data.

Purpose

Establish procedures for user account management of information systems, products or services including granting, reviewing, inactivation, updating or terminating access for USG administrators, executives, faculty, staff, researchers, clinical care providers and students. These procedures also apply to individuals or representatives of entities in relationship through formal, informal, contract or other types of agreements who interact with USG information systems, products, or services.

Procedures

- USG organizations shall identify and categorize information systems, products or services that process or store confidential or sensitive information or are mission-critical systems. The suggested responsible party is the system owner.
- USG organizations will identify the system owner and data steward for each mission-critical system, products or service containing confidential or sensitive information. A list of these systems, products or services and the associated owners shall be made available upon request. The suggested responsible parties are the system owner and data steward.
- USG organizations will maintain an up-to-date mapping of users to information systems, products or services. The system owner will provide the data steward with user ID information. The suggested responsible parties are the system owner and data steward.
- Only authorized users should be allowed physical, electronic or other access to information systems, products or services.

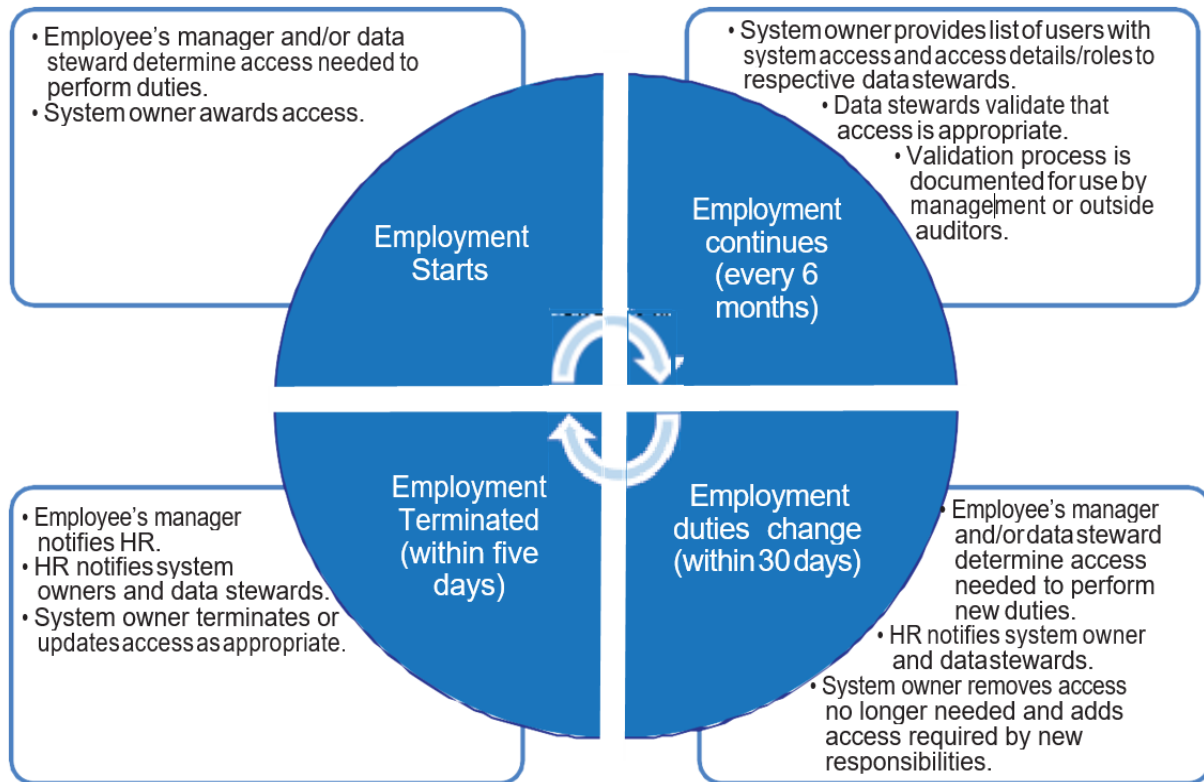


Figure 2: Recommended Process Flow

- USG organizations will define both administrative and technical access controls to address cybersecurity and data privacy concerns. The suggested responsible parties are HRM, the system owner and data steward. Access controls must include, but not limited to:
 - Documented procedures to grant, review, deactivate, update or terminate account access.
 - Ensure appropriate resources are available and maintained to adequately authenticate and verify authorized access.
 - Ensure appropriate resources are available and maintained to prevent and detect unauthorized use.
- System owners, data stewards and users share the responsibility of preventing unauthorized access to USG organizations' information systems, products or services.
- Data stewards will analyze user roles and determine level of access required to perform a job function. The level of authorized access must be based on principle of least privilege (POLP).
- HRM and data stewards will notify the system owner of personnel status changes in job function, status, transfers, referral privileges or affiliation. The suggested responsible parties are the system owner, data steward and HRM.
- Access to an information system must be reviewed regularly. Data stewards must review user access to the information system every six months and document findings with the system owner.

- System owners will update information system access no more than five business days after terminations and no more than 30 days after other personnel status changes.

3.1.2 Managing Multifactor Authentication

Securing information and information systems, products or services remains a core responsibility of the University System of Georgia (USG). USG organizations maintain a legal and ethical responsibility to protect information in its care. Organizations using only single sign-on authentication are no longer secure and at risk of compromise. To mitigate this risk, multifactor authentication (MFA) must be implemented across the USG.

Organizations without MFA must develop a plan of action to implement this authentication service to reduce the risk of account compromise by mitigating the weakness of single-factor authentication. USG Cybersecurity will be tracking the implementation of MFA.

Plans of Action

Elements of the organization's MFA plan of action shall include deployment priorities (roadmap), personnel affected, and configuration baselining.

Deployment Priorities: Deployment may be implemented using a tiered approach beginning with:

1. Systems, products or services storing critical (protected) information. Examples of these systems, products or services include and are not limited to mission-critical systems, OneUSG, databases and warehouses, email and internet facing web servers and portals.
2. Systems, products or services permitting privileged access (e.g. administrator roles), remote access, servers critical to supporting business function and all single sign-on systems.
3. All remaining systems, products or services supporting the organization.



Figure 3: Multi-Factor Authentication

Personnel Affected: Any faculty, staff, student, affiliate and contractor that has access to any protected USG or third-party managed resource.

Configuration Baselining: Securely configure MFA to limit legacy protocol bypass, direct local access and protocols that weaken the safeguards effectiveness. Additional setting to harden should be considered, for example: push notification versus call or passcode, US versus non-US connectivity, and time-out limits.

Goal

USG organizations shall request Employee Self Service (ESS) features to be enabled once MFA protection is implemented for OneUSG. Following that, MFA shall be the standard for accessing all USG or third-party managed resources by all USG employees, students, affiliates and contractors.

Section 3.2 Log Management

3.2.1 Purpose

Logs contain information related to many different types of events occurring within systems, products or services, networks and applications. Logs serve functions such as optimizing system and network performance, recording the actions of users and providing data useful for investigating security events. Logs containing records related to computer security, may include audit logs that track user authentication attempts and security device logs that record possible attacks. These requirements address security-related logs and log entries.

A fundamental problem with log management occurring in many organizations is effectively balancing a limited quantity of log management resources with a continuous supply of log data. Log generation and storage can be complicated by several factors: including a high number of log sources, inconsistent log content, formats, timestamps among sources and increasingly large volumes of log data. Log management also involves protecting the confidentiality, integrity and availability of logs. This challenge can be mitigated in part by implementing the principle of data minimization – log only what is necessary. The dominant problem with log management is ensuring that cybersecurity, system and network administrators regularly perform effective analysis of log data.

3.2.2 Objective

Establish the requirements for computer and network resource log management for the USG organizations computing and network environment. The goals of log management are:

- Define the criteria for log generation, log transmission, log storage and disposal.
- Proactive maintenance of information system resources.
- Awareness of “normal” vs. “abnormal” network traffic or system performance.
- Support after-the-fact investigations of cybersecurity incidents.

3.2.3 Standard

USG resources that store, access or transmit data and categorized as “HIGH” or “Mission-Critical System” shall be electronically logged. Logging shall include system, application, database and file activity whenever available or deemed necessary.

USG organizations must formalize log management by:

- Creating and maintaining a secure log management infrastructure by balancing system performance, storage resources and legal requirements;
- Committing resources to perform timely log review and analysis about access, change monitoring, malfunction, resource utilization, security events and user activity;
- Identifying roles and responsibilities of staff associated with this process;

- Developing standards, procedures and guidelines as needed to support this program. Reviewing audit logs minimally every 30 days during system reviews;
- Prioritizing log management; and,
- Describing log lifecycle process from defining preservation, legal holds, and regulated retention requirements to disposal and verification.

The following table provides recommendations of logging configuration types. Moreover, USG organizations should not adopt these values as-is, instead use them as a starting point for determining what values are appropriate for their needs.

Table 3.3: Logging Configurations

Category	Low Impact Systems	Moderate Impact Systems	High Impact Systems
Log retention	1 to 2 weeks	1 to 3 months	3 to 12 months
Log data analyses frequency (through automated or manual means)	Every 1 to 7 days	Every 1 to 3 days	Once a day

Section 3.3 Continuity of Operations Planning

3.3.1 USG Continuity of Operations Planning Standard

Purpose

Continuity of operations planning ensures the continuity of business and essential functions through a wide range of emergencies and disasters including localized acts of nature, accidents and technological or attack-related emergencies to ensure that at minimum the general support systems continue to operate and be available.

Guiding Principles

- The USG *Continuity of Operations Plan* (COOP) shall be developed following existing standards, industry best practices, Federal Information Security Management Act (FISMA), Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST) guidelines, USG Cybersecurity tools and templates.
- The USG COOP will require the involvement of all USG organizations to ensure an effective USG response to contingencies and disasters.
- The USG COOP must incorporate the physical and logistical limitations of the USG operating locations.
- The USG COOP will be aligned with and operationalize the USG *Emergency Operations Plan* and the Enterprise Risk Management Program.

Standard

Recovery strategies must be developed for IT systems, products, or services. This includes network connectivity, servers, data and support systems. Priorities for IT recovery must be consistent with the priorities for recovery of network connectivity and other critical processes that were developed during the operational impact analysis. All USG IT organizations must:

- Create, implement, maintain and test a continuity of operations plan – COOP, that will allow appropriate response to a wide range of contingencies and disasters that may occur at all USG organizations.
- Describe the actions to be taken before, during and after events that disrupt critical information system operations.
- All plans must be tested every 24 months and evidence of testing must be available upon request, and part of the continuity of operations plan documentation.
- All recovery planning must include lessons learned and update recovery strategies.

The formal COOP and processes must at minimum include:

- The backup and recovery processes, and plan for critical general support systems.
- A cyber incident response process and plan.
- A disaster recovery plan for critical general support systems.

Each USG organization must keep its COOP up-to-date and provide a COOP status report annually via the Cybersecurity Program Report (CPR). It is important to adapt the detailed content of each plan section to suit the needs of the individual USG organization, with the understanding that disaster recovery plans (DRP) are based upon available information so they can be adjusted to changing circumstances.

General Support System

A general support system (GSS) is an interconnected or dependent set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- Backbone (e.g., network core);
- Communications network;
- USG organization data processing center, including its operating system and utilities; or,
- Shared information processing service facility (data center).

A GSS should have a Federal Information Processing Standard Publication (FIPS) 199 impact level of low, moderate or high in its security categorization depending on the criticality or sensitivity of the system, and any major applications the general support system is supporting. A general support system is considered a major information system when special management attention is required, there are high development, operating or maintenance costs; and the system/information has a significant role in the administration of USG organization's programs. When the general support system is a major information system, the system's FIPS 199 impact level is either moderate or high. A major application can be hosted on a general support system.

Minimum Continuity of Operations Plan Content (can be separate processes and plans)

- *Backup/Recovery and Off-site Storage of Critical Data and Systems*

Create, implement, maintain and test a backup and recovery process that will allow appropriate response to a wide range of contingencies and disasters that may occur within the USG. Backup and retention schedules and procedures are critical to the recovery of USG organization's

systems, products or services, and data. The detailed procedures for such a recovery should include hardware, software (including version), data file backup and retention schedules, off-site storage details, and appropriate contact and authority designation for personnel to retrieve media. Store backup materials and media at suitable off-site locations. For locations where off-site storage is not practical or cost effective, COOP leadership will designate an appropriate facility to serve as the off-site storage of backup media. A suitable facility is one within reasonable distance of the main campus or facility, but not likely to be immediately threatened by the contingency or disaster.

- *Cyber Incident Response Capability*

The USG organization will establish a cybersecurity incident response capability program to respond to and manage adverse activities or actions that threaten the successful conduct of teaching, instruction, research and operations in the USG. The cybersecurity incident response plan will follow existing USG policies, standards, cybersecurity tools, industry best practices and International Standards Organization (ISO) or NIST guidelines. The USG organization's management must promptly investigate incidents involving loss, exposure, damage, misuse of information assets or improper dissemination of information. All USG organizations are required to report information security incidents consistent with the security reporting requirements in the cybersecurity incident management standard. Proper incident management includes the formulation and adoption of a written incident management plan that provides for the timely assembly of appropriate staff that can develop a response to, appropriate reporting about and successful recovery from a variety of incidents. In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences in the future.

- *Disaster Recovery Management*

Each USG organization must establish a disaster recovery plan for information systems, products or services categorized as critical, that provides processes supported by executive management and resources to ensure the appropriate steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans and ensure the USG organization has the ability to continue its essential functions during a business disruption or major catastrophic event and to provide timely communication. The program controls ensure that information is protected by providing for regular backup of automated files and databases, identifies and reduces risks, limits the consequences of the incident, and ensures the availability of information assets for continued business. The communication controls (RC.CO – involving restoration activities) ensure that information concerning recovery are provided to internal and external stakeholders, executive and management leadership (e.g., USO, ITS, Cybersecurity) to inform and manage public relations for the purpose of repairing reputation post-incident.

- *Disaster Recovery Planning*

Disaster recovery planning provides for continuity of computing operations that support critical business functions, minimizes decision-making during an incident, produces the greatest benefit from the remaining limited resources, and achieves a systematic and orderly migration toward

the resumption of all computing services within a USG organization following a business disruption. It is essential that critical IT services and critical applications be restored as soon as possible. It is significant to recognize that no disaster recovery program is ever complete. All disaster recovery planning is based upon available knowledge and assumptions and must be adapted to changing circumstances and business needs, as appropriate. Strategies, procedures and resources must be adapted as often as necessary to recover critical applications. Recovery strategies must be developed and updated routinely to anticipate risks including loss of utility (e.g., hardware, software, power, and telecommunications), loss of access to the facility and loss of facility. Also, avoid the typical scenario planning approach that calls for separate plan for each “what-if” scenario. Instead, develop one plan that can be adapted to different scenarios, which also reduce the effort to maintain the *Disaster Recovery Plan (DRP)/Business Recovery Plan (BCP)*. The disaster recovery planning process supports necessary preparation to identify and document procedures to recover critical operations in the event of an outage. USG organizations should consider the results of their risk analysis process and their business impact analysis when developing their DRP. Each USG organization’s processes should culminate in a viable, fully documented, and tested DRP. To improve the likelihood for the full recovery of key business processes, DRPs should be developed as part of a complete business continuity (BC) program, which includes emergency response and business resumption plans.

Applicability and Compliance

This standard applies to all USG information resources, systems, products, or services and to all users of these resources, systems and technology within the USG information infrastructure. Compliance with this standard is mandatory.

Section 3.4 Network Services

3.4.1 Network Services Standard

Purpose

PeachNet®, USGs statewide network, is the foundation that enables efficient, robust access to mission-critical online learning resources, business applications and transactions, and academic research. The transformation to the “Information Age” continues to be revolutionary in its impact on higher education. Students, researchers and administrators have come to view the network as a tool to enhance their learning experience.

Standard

PeachNet services are governed by the BOR of the USGs *PeachNet Acceptable Use Policy*. In addition, the following outlines the roles and responsibilities of ITS and USG Organizations:

ITS Network Services

- Regional Wide Area Networks (WANs)
 - ITS will facilitate the construction and management of Regional WANs to provide managed telecommunications services to the physical addresses of USG locations.
 - The bandwidth delivered to each location, unless explicitly defined, will be provisioned based on utilization and trend-analysis data.

- ITS will maintain the fiber infrastructure to support USG Regional WANs.
- ITS will provide each location with public IP address ranges based on site needs and requirements.
- Internet and Internet 2
 - ITS will provide Internet and Internet 2 access to all USG locations.
 - ITS will require and establish appropriate Service Level Agreements (SLA) from Service Providers for any contracted network services. These SLAs will be established in accordance with normal industry standards for network-based performance measurements. ITS will also perform continuous network monitoring and service management to capture availability, performance and utilization statistics.

USG Institutional Responsibilities

- USG organizations will provide Co-Location facilities allowing ITS to create a PeachNet Point of Presence to support interconnections for Regional USG WANs, the Internet and Internet 2.
- USG organizations will provide necessary power to support USG Regional WANs equipment within the PeachNet POP facilities.
- USG organizations shall have the ability to accept and utilize the physical interface specified and delivered by ITS.
- USG organizations are responsible for the oversight and distribution of the public Internet Protocol address assigned to each institution by ITS.
- USG organizations will be responsible for providing ITS with local administrative and technical contacts.

Firewall services at a statewide, regional or district level are excluded from this section.

- USG organizations are responsible for implementing and managing a campus security architecture and may consist of devices such as firewalls, intrusion detection/prevention, content filters, etc.

Section 4. Financial and Human Resource Management

Section Control

Table 4.1: Revision History

Date	Description of Change
04/18/2016	Section 4.1 - added a statement to the IT Procurement Policies. Revised cost estimate.
05/02/2016	Initial redesign referenced in a new structure and format. PDF, structure and format.
11/17/2016	Section 4.1 – updated spending limits for purchases more than \$1 million. Spending limits updated.
01/08/2021	Section 4.1 – updated spending limits tier structure. Spending limits updated.

Table 4.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date

Introduction

Sound management principles are required for the budget and human resources allocated to the CIO and centralized IT organization. In the event any standards defined in this manual conflict with the USG BOR policy or procedures as defined in other relevant guides such as the Fiscal Affairs BPM, those documents take precedence.

A financial management framework that encompasses cost, benefits, prioritization within budget, a formal budgeting process and management against the budget should be established and maintained to manage IT-enabled investment programs and projects. Stakeholders should be consulted to identify and control the total costs and benefits within the context of the IT strategic and tactical plans and initiate corrective action where needed.

A competent workforce should be acquired and maintained for the creation and delivery of IT services to the organization. This is achieved by following defined and agreed-upon practices for recruiting, training, evaluating performance, promoting and terminating personnel.

Section 4.1. Technology Procurement Approval Process

Authority for processing technology procurements is assigned to the Georgia Technology Authority (GTA) through the Official Code of Georgia Annotated (O.C.G.A § 50-25). In the same chapter (O.C.G.A § 50-25-1), the USG is specified as being exempt from this legislation. The establishment of the GTA intersected with the authority of the Department of Administrative Services (DOAS), which resulted in a memorandum of understanding between the GTA, DOAS and the USG in 2007, granting delegated authority, with some constraints, for technology procurements to the USG CIO).

Section 10.3 of the BOR *Policy Manual* delegates authority from the BOR to the USG CIO to approve USG technology procurements on their behalf. Section 10.3 authorizes the USG CIO to further delegate

approval authority to institution presidents or their designee(s). This section of the *USG IT Handbook* implements this BOR policy.

4.1.1 Spending Limits

The USG CIO delegates approval authority for individual IT purchases according to the following limits:

1. \$500,000: Georgia Institute of Technology, Augusta University, Georgia State University, Kennesaw State University and the University of Georgia.
2. \$250,000: Columbus State University, University of North Georgia, Georgia Southern University, , University of West Georgia and Valdosta State University.
3. \$100,000: All other USG organizations.

4.1.2 IT Procurement Policies

1. IT is defined in Section 10.1, General Policy on Information Technology, of the *BPM*.
2. Procurement of technology-related goods and services should follow the relevant *BPM* procedures.
3. Authorization is not required for activities that are part of normal maintenance of an existing system.
4. Any purchase of software that necessitates an inbound data interface with any hosted or centrally supported USG enterprise application must be approved by the USG CIO.
5. Purchases for goods or services that are likely to have a significant impact on the wide area network bandwidth allocated to the institution should be carefully planned with the USG CIO.
6. Externally approved, grant-funded technology purchases that do not interact with USG enterprise applications or USG enterprise networks may be approved by the institution president or his or her designee for IT purchases.
7. Institutions may not divide large purchases into smaller packages to avoid the need for USG approval. Individual purchases that are below these amounts but are part of a larger initiative that will eventually exceed these amounts, shall also require written USG CIO approval (e.g., purchases of microcomputers for various lab locations on a campus even if the purchases are for different buildings and from multiple fund sources.)
8. USG CIO approval of IT requests will expire one year after being granted.
9. If there is a revised cost estimate to a previously approved IT procurement request and that estimate increases by more than 10%, a new IT procurement approval must be obtained.
10. Purchases over \$1 million will require a business case to be submitted for review and approval.

4.1.3 Requesting Approval

IT requests requiring USG CIO approval must be submitted via the SharePoint CIO Advisory Council Team Site by following the USG IT Purchase Approval link in the left-hand menu. If the purchase is over \$1 million, the business case template shall be downloaded, completed, and attached to the purchase approval request.

The USG CIO normally approves IT requests within four (4) business days of receipt. Business cases will require a longer period depending on the amount of communication, coordination, and vetting that needs to take place. Institutions should plan appropriately.

Section 4.2 Financial Management

A financial management framework for the centralized IT budget and the overall spend on IT across the organization should be established. Ideally, the IT Shared Governance process would incorporate some degree of budget review that includes the cost and benefit analysis of major planned expenditures, a budget request process and a method of expense monitoring throughout the year.

Section 4.3 Human Resource Management

A competent workforce is required for the creation and delivery of effective IT services to the organization and requires close coordination with the Human Resources (HR) office. The workforce management responsibilities delegated to the line managers of the IT organization should be guided by defined and agreed- upon practices for recruiting and retaining staff. This should include a training plan, routine performance appraisals and clear criteria for promotions and disciplinary actions. This process is critical since the creation and delivery of IT services are heavily dependent on the motivation and competence of IT personnel.

Section 5: Cybersecurity

Section Control

Table 5.1: Revision History

Date	Description of Change
05/02/2016	Initial Redesign – Referenced in a new structure and format. PDF, structure and format
05/17/2016	Section 5.12.3 – Added a statement about system-level passwords. System-level password information added in bullet number 4.
11/03/2016	Section 5.13 – Content in section was updated and revised. Revised Domain Name System
11/03/2016	Section 5.13 – Added link to the revised Domain Name System (DNS) Guidelines. Domain Name System Guidelines
05/15/2017	Section 5.3 – Revised section for consistency in format and content. Deleted table. Added “USG organizations” as stated in the Introduction section, changes made to the USG Incident Response and Reporting Standard and deleted Incident Categories and Reporting Timeframes table.
05/15/2017	Section 5.10 – Revised section for consistency in format and content. Added content for clarification.
09/07/2017	Section 5 – Reviewed and revised entire Section 5 for consistency of content. Added “USG organizations” as stated in the Introduction section and other minor editorial changes removing policy and standard where appropriate.
09/07/2017	Section 5 – Incorporated revisions in Section 5 by University of North Georgia. Incorporated minor editorial changes recommended by University of North Georgia.
01/02/2019	Section 5.10 – Align with the NIST framework and FIPS. Revisions to required security reporting activities with corresponding due dates. Changed ISPR to CPR and revised components. New sub section “Remediation and Mitigation Tracker” added.
02/24/2020	Section 5.3 – Incident Management. Updated language, added baseline requirements and template to submit a plan for review.
02/24/2020	Section 5.9 – Awareness Training. Updated language to align with Section 5.10.
02/24/2020	Section 5.10 – Required Reporting. Updated language and diagram to include biannual awareness training requirements.
02/24/2020	Section 3.1.2 – Multifactor Authentication. Added section to standardize MFA deployment across the USG enterprise.
04/30/2020	Section 5.1.1 – editorial change, and cybersecurity framework (CSF) alignment. Add “continuous”
04/30/2020	Section 5.1.2 – editorial change, and CSF alignment. Add bullet 3 “expected dataflow diagrams,” and add bullet 4 “expected dataflow diagrams,”
04/30/2020	Section 5.1.2 – editorial change, and CSF alignment. Editorial corrections #6, add “principle of least function...”
04/30/2020	Section 5.3.1 – editorial change, and CSF alignment. Add list “i. – v.” to # 5 and add “incident alert thresholds” to #6
04/30/2020	Section 5.5 and 5.5.2 – editorial change, and CSF alignment. Add “continuous,” add “5.5.2 - Event data (logs) shall be collected and correlated from sources and sensors.” Add “both internal and external to the organization” and add definition “Risk Register”

04/30/2020	Section 5.5.5 – editorial change, and CSF alignment. Add “Continuously monitor...” and add “, which includes:” and list “a. – d.”
04/30/2020	Section 5.10.1 – editorial change. Renumber Figure to 4/relocate reference to bottom
04/30/2020	Section 5.11.7 – editorial change, and CSF alignment. Add “Principle of least function...”
04/30/2020	Section 5.13 – editorial change. Rebrand section title to “Domain Name System Management”
04/30/2020	Section 5.14 – editorial change, and CSF alignment. Rebrand section title to “Information Protection Management.” Strike space in 1st paragraph, strike “of this manual”, and add “program’s protection processes will:”. Add “To improve the protection processes, ensure...” and add “information protection/”
04/30/2020	Section 5.14.5 – editorial change, and CSF alignment. Add “or protocols” and “or protected” and “Cybersecurity” and strike “Information & ePrivacy”
07/08/2020	Incorporate cybersecurity charter verses publishing another document. Replace “Introduction” with new “USG Cybersecurity Charter”
07/09/2020	Section 5.1 – editorial changes and alignment with the CSF and privacy framework (PF). Remove existing 5.1 introductory paragraph – information was used in Section 5 Charter, replace with new 5.1 introductory paragraph, and change current old 5.1.1 heading to 5.1.2, leaving 5.1.1 open. Also, fill open 5.1.1 space with 5.1.1 Cybersecurity Program Plan Requirements, strike opening sentence and replace with 5.1.2 USG Organizational Responsibilities, and change current old 5.1.2 heading to 5.1.3. Lastly, insert content into sentence 4, Section 5.1.3 and change current old 5.1.3 heading to 5.1.4.
07/09/2020	Sections 5.3 through 5.14 – editorial changes and alignment with the CSF and PF. Insert new Line “g.” to Section 5.3.1, Edit Section 5.3.3, edit Sections 5.4.1 and 5.4.2, insert new content Section 5.5.2, insert new content Section 5.5.5, strike: “Note: The definition of Data owner....” In Section 5.6.2, add “critical system” paragraph at end of Section 5.6.2, insert opening and closing sentences to Section 5.8.2, insert new Section 5.8.5, update Section 5.9.1, insert new Section 5.11.8 Segmentation, add opening sentence to Section 5.14, and edit opening sentence for Section 5.14.2 and add Step 9 and content.
09/16/2020	Section 5.3 – addition. Added Georgia Cybersecurity Board notification requirement.
01/08/2021	Consolidated organizational, roles and responsibility language into one section. Section 5.1 – Consolidated and updated 5.1 & 5.2, removing 5.1.4 to become 5.2.
01/08/2021	Elevated AUP into stand-alone section. Section 5.2 – Elevated 5.1.4 to new 5.2 AUP
06/30/2021	Section 5.2 – adjusted terms. Section 5.2.1, 3. e) updated to align with 1 st Amendment interpretation.
07/23/2021	Sections 5.3 and 5.5 – added/updated language to include legislation changes and supplier management.
07/27/2021	Section 5.7 and 5.12 – add/update PII definition and update password management standard.
08/23/2021	Sections 5.14, 5.15, 7.1 and 10 – removed redundant language; updated email use and retirees; add physical security and shift from on-prem to cloud service.

Table 5.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date	Revision Date(s)
5.0	USG Cybersecurity Charter	July 2020	August 2020	August 2020	July 2020

5.1	USG Cybersecurity Program	February 2009	February 2009 to Cybersecurity February 2013 to IT Handbook	February 2009	July 2020
5.2	Cybersecurity Organization and Administration	February 2009	February 2009 to Cybersecurity February 2013 to IT Handbook	February 2009	May 2014
5.3	Incident Management	December 2008	December 2008 to Cybersecurity February 2013 to IT Handbook	February 2009	July 2020
5.4	USG Information Asset Management and Protection	July 2013	May 2014	TBD	July 2020
5.5	IT/IS Risk Management	April 2010	April 2010 to Cybersecurity February 2013 to IT Handbook	April 2010	July 2020
5.6	USG Information System Categorization	June 2013	May 2014	July 2014	July 2020
5.7	USG Classification of Information	June 2013	May 2014	July 2015	July 2015
5.8	USG Endpoint Security	June 2013	May 2014	July 2015	July 2020
5.9	Security Awareness, Training, and Education	April 2009	April 2009 to Cybersecurity February 2013 to IT Handbook	April 2009	July 2020
5.10	Required Reporting	April 2009	April 2009 to Cybersecurity February 2013 to IT Handbook	April 2009	February 2020
5.11	Minimum Security Standards for USG Networked Devices	October 2008	October 2008 to Cybersecurity May 2014 to IT Handbook	October 2008	February 2020
5.12	Password Security	July 2010	July 2010 to Cybersecurity February 2013 to IT Handbook	July 2010	May 2014
5.13	Domain Name Service	February 2011	February 2011 to Cybersecurity February 2013 to IT Handbook	February 2011	May 2014
5.14	Identity Theft Prevention Standard - Red Flags Rule	January 2011	January 2011 to Cybersecurity May 2014 to IT Handbook	January 2011	July 2020
5.15	Email Use and Protection	January 2009	January 2009 to Cybersecurity May 2014 to IT Handbook	May 2014	May 2014
5.2.2	Mobile Workforce Requirements	March 2021	March 2021	March 2022	March 2021

USG Cybersecurity Charter

Introduction — University System of Georgia (USG) Cybersecurity is an operational program providing advice and guidance in developing processes, selecting technologies and training USG personnel. To advance the role of advice and guidance, the USG chief information security officer (CISO) coordinates the efforts of the USG organizational information security officers (ISOs) primarily through the publication of the USG *IT Handbook*; through biannual program reviews, compliance reports, mandatory awareness training, and ISO meetings; and through participation in the Chief Information Officers

Advisory Council (CIOAC). USG Cybersecurity's mission statement is "Develop and maintain an affordable and efficient enterprise cybersecurity organization to identify and reduce risk." This document presents the philosophy of cybersecurity within the USG and represents the endorsement of USG's executive leadership. IT identifies the motivation for cybersecurity, describes cybersecurity goals, and defines the scope of cybersecurity roles and responsibilities.

Authorization — *Board of Regents (BOR) Policy Manual*, Section 10.4. states, "The USG CISO shall develop and maintain a cybersecurity organization and architecture in support of cybersecurity across the USG between USG institutions. The USG chief information security officer shall maintain cybersecurity implementation guidelines that the USO, all USG institutions, and the GPLS shall follow in the development of their individualized cybersecurity plans." To the extent permitted by law, USG Cybersecurity is authorized to review and appraise all operations, policies, plans and procedures concerning cybersecurity and the functions supporting cybersecurity. Documents and other materials provided to USG Cybersecurity will be handled in the same prudent manner as handled by those employees normally accountable for them.

Motivation — USG recognizes that information and IT assets are critical business assets. It is the responsibility of all users to ensure the safeguarding of business assets. USG implements, maintains and monitors a comprehensive enterprise cybersecurity and compliance program. USG values the ability to openly communicate and share information. USG information (whether belonging to USG or held in trust on behalf of its clients and business partners) is an important asset that shall be protected according to its value and the degree of damage that could result from its misuse, unavailability, destruction, unauthorized disclosure or modification. Improper disclosure or destruction of these assets may result in harm to the USG. Information assets are identified, valued, assessed for risk and protected as appropriate to the needs and risks of the business.

Cybersecurity Goals — Cybersecurity is a risk management discipline addressing the preservation of information confidentiality, integrity and availability, which is established via a hierarchical set of policies, standards and procedures that help users and administrators define and mitigate risks, maintaining a trade-off between information value and cost of risk mitigation. The goals are:

- Provide processes, standards and guidelines that promote an enterprise cybersecurity environment.
- Improve cybersecurity by implementing a "defense-in-depth" architecture with the focus on proactive detection.
- Prioritize cybersecurity at all levels of the enterprise.
- Promote the importance of cybersecurity awareness, training and education system wide.
- Inform the ISOs, CIOs, and USO leadership of the state of cybersecurity maturity across the USG enterprise.

Scope — Data and information is protected in whatever media, including, but not limited to, paper documents and electronic or digital formats. Data and information should be protected while at rest and when it is handled, transmitted or conveyed. IT assets include all devices and hardware and/or software components of the IT infrastructure, applications and data stores. This charter applies to all USG employees, affiliates and contractors that have access to USG resources.

Roles/Responsibilities

- Executive Leadership — Executive leadership shall establish strategic direction, define risk appetite, be accountable for cybersecurity and ensure compliance with security policies, standards, procedures and practices within their respective organization’s areas of responsibility.
- USG Chief Information Security Officer (USG CISO) and USG Cybersecurity shall —
 - Create a cybersecurity program that ensures the confidentiality, integrity and availability of its information assets.
 - Provide oversight and guidelines for administration of cybersecurity policies, processes, and procedures and will consider the effects of security requirements on the USG enterprise by maintaining sections concerning data governance, management and privacy of the *Business Procedures Manual* (BPM) and all sections concerning cybersecurity of the *USG IT Handbook*.
 - Design, implement and maintain an enterprise security operations center (ESOC) that monitors University System Office (USO) and USG networking assets for evidence of cybersecurity events or incidents.
 - Promote communications within the USG and third-party partners to share a broad cybersecurity situational awareness and express the effectiveness of protection technologies.
 - Coordinate USG responses to information and information systems breaches and other cybersecurity incidents
 - Represent cybersecurity interests in and provide expertise and governance to USG/USO working groups, e.g. USG Enterprise Risk Management (ERM), Data Privacy, Data Governance and Management, and CIOAC.
 - Liaison with the state CISO and other external officials to keep them informed of significant cybersecurity incidents.
 - Report significant cybersecurity issues directly to the Executive Vice Chancellor of Administration and to the Chancellor.
 - Lead USG organization’s cybersecurity functions of cyber-specific areas as needed to fulfill the system-wide cybersecurity plan.
- Users of USG resources — Cybersecurity is everyone’s responsibility. Users are required to abide by this charter and subsequent standards and procedures. All have a responsibility to report suspected cybersecurity failures or policy violations as defined within the *USG IT Handbook*.

To operationalize the Charter, all USG organizational CIOs/ISOs shall implement the standards and directives located within the *BPM* and *USG IT Handbook*.

Section 5.1 USG Cybersecurity Program

USG organizations must ensure mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity and data privacy roles, responsibilities and risk management decisions, which are used in developing cybersecurity plans. The *Board of Regent’s Policy Manual*, Section 10.4 states, “The USO, all USG institutions, and the GPLS shall each develop, implement, and maintain a cybersecurity plan consisting of cybersecurity policies, standards, procedures

and guidelines that is consistent with the guidelines provided by USG Cybersecurity and submit the plan to USG Cybersecurity for review upon request.”

5.1.1 Cybersecurity Program Plan Requirements

USG Cybersecurity created a rubric to provide guidance in the development of a standardized cybersecurity plan – CYBERSECURITY PROGRAM PLAN RUBRIC: PHASE I (Standards for Safeguarding Customer Information; Final Rule 16 CFR Part 314 as required by Department of Education, Federal Student Aid - Section 4: Elements. Additional elements have been drawn from NIST SP800-53 Rev 4 Information Security Program.) The rubric consists of the following information:

The USG organization shall develop, implement, maintain and disseminate a written cybersecurity program plan that...

1. Provides an overview of the requirements for the cybersecurity program and a description of the cybersecurity program management safeguards (controls).
 - (a) Designates a trained and dedicated Information Security Professional to implement the plan.
 - (b) Defines how internal and external risks are identified.
 1. Establishes data management lifecycle procedures.
 2. Introduces risk assessment that considers identification, protection, detection, response and recovery plans.
 - (c) Designs and implements cybersecurity safeguards to control the identified risks.
 1. Designs and implements a response plan.
 2. Regularly monitors the safeguard effectiveness.
 3. Defines notifying USG/USO in the event of a data breach when appropriate.
 - (d) Oversees third party systems, products and service providers to implement and maintain safeguards.
 - (e) Reviews, evaluates, adjusts and updates the Cybersecurity Plan annually.
 1. Protects the Cybersecurity Plan from unauthorized disclosure and modification.
 2. Approves plan by senior official with accountability and authority.
2. Implements biannual and mandatory awareness training to all employees.

5.1.2 Information Security Officer (ISO)

USG organizations must identify an ISO who will be responsible for establishing, maintaining, and reporting on cybersecurity roles, responsibilities, policies, plans, processes and procedures. In accordance with the *BOR Policy Manual*, Section 10.4.2, USG organizations, “shall include maintaining a trained and dedicated information security officer.” The ISO’s contact information must be sent annually to USG Cybersecurity, as noted in Section 5.10 of this Manual.

5.1.3 USG Organizational Responsibilities

USG organizations, utilizing the appointed and designated ISO, shall create a cybersecurity program that ensures the confidentiality, integrity, and availability of USG information assets. USG organizations shall develop and implement a governance structure that enables an ongoing understanding of the

organization's risk management priorities. The program will have oversight for administration of cybersecurity standards, processes and procedures, and will consider the effects of cybersecurity requirements on the entire enterprise. Every cybersecurity requirement will be tied to an operational need, a state or federal regulation or an industry standard practice. The policies, processes and procedures to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the organization's management of cybersecurity and data privacy risk.

Furthermore, the USG organization will interpret state or federal regulations and apply their requirements to USG information resources, administer organizational programs and execute projects to meet cybersecurity objectives. Additionally, liaison functions shall be performed between USG organizations and the USG for matters regarding cybersecurity and privacy. USG organization can accomplish this by ensuring policies, processes and procedures (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated. Accordingly, USG organizations must:

1. Build a cybersecurity program and program plan, which includes policies, processes and procedures;
2. Assign management roles and responsibilities for the cybersecurity program, including the appointment of an Information Security Officer (ISO);
3. Evaluate local infrastructure compliance with cybersecurity policies, processes, standards and procedures;
4. Establish processes and procedures for access to sensitive information systems, products or services;
5. Establish processes and procedures to minimize the likelihood of disruptions, to recover from disasters and to respond to cybersecurity incidents;
6. Develop and maintain a computer/data incident management component;
7. Develop and maintain a program to manage and protect information assets;
8. Establish and maintain an information technology and cybersecurity risk management program, including a risk assessment, analysis, planning mitigation, and a continuous monitoring process;
9. Categorize information systems, products, or services and classify information records (data);
10. Implement the minimum endpoint security standard requirements/capabilities;
11. Maintain a biannual cybersecurity awareness, and training component for all employees and contractors;
12. Comply with USG reporting requirements;
13. Implement minimum security standards for networked devices;
14. Implement password security controls;
15. Implement and administer domain name security; and
16. Make reasonable efforts to manage information consistent with the organization's risk strategy to reduce cybersecurity risks, protect individuals' privacy, increase manageability and enable the implementation of privacy principles.

5.1.4 Policy and Procedure Management Requirements

Policy provides management direction for USG organizations to conform to business requirements, laws and administrative directives and mandates. Procedures are the specific series of actions that are taken to comply with policies and standards. In addition, standards are the specifications that contain measurable, mandatory rules to be applied to a process, technology and/or action in support of a policy. The USG *IT Handbook* is a standard.

A “standard of due care” is required to prevent misuse or loss of USG information assets. USG organizations must provide for the integrity and cybersecurity of its information assets. To demonstrate this due care, USG organizations must...

1. Establish and maintain management and staff accountability for protection of USG information assets.
2. Establish and maintain processes for the assessment and analysis of risks associated with USG information assets.
3. Establish and maintain cost-effective risk management practices intended to preserve the ability to meet USG program objectives in the event of the unavailability, loss or misuse of information assets.
4. Develop and implement a vulnerability management plan that includes, but is not limited to...
 - (a) Conduct continuous monitoring to identify and verify the effectiveness of implemented protective measures, e.g. vulnerability scanning.
 - (b) Technology upgrades, which include, but are not limited to, operating system upgrades on servers, routers and firewalls. Appropriate planning and testing of upgrades must be addressed, in addition to departmental criteria for deciding which upgrades to apply.
 - (c) Security patches and security upgrades, which include, but are not limited to, servers, routers, desktop computers, mobile devices and firewalls. Application and testing of the patches and/or security upgrades must be addressed, in addition to departmental criteria for deciding which patches and security upgrades must be applied and how quickly.
 - (d) Intrusion Prevent System (IPS)/firewall configurations to detect anomalous activity in a timely manner to understand potential impacts. Documentation of the baseline configuration is a requirement for each IPS/firewall with expected dataflow diagrams, updates of the documentation for all authorized changes and periodic verification of the configuration to ensure that it has no changes during software modifications or rebooting of the equipment.
 - (e) Server configurations, which must clearly address all servers that have any interaction with Internet, extranet or intranet traffic. Creation and documentation of a baseline configuration for each server with expected dataflow diagrams, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment must be required.
 - (f) Server hardening, which must cover all servers throughout the organization, not only those that fall within the jurisdiction of the organization’s IT area. The process for making changes based on newly published vulnerability information as it becomes available must be included. Principles of least functions must be implemented. Further, this must address, and

be consistent with, the organization's policy for making security upgrades and security patches.

- (g) Software management and software licensing, which must address acquisition from reliable and safe sources and must clearly state the organization's policy about not using pirated or unlicensed software.
- 5. Ensuring that the use of peer-to-peer technology for any non-business purpose is prohibited. This includes, but is not limited to, transfer of music, movies, software and other intellectual property. Business use of peer-to-peer technologies must be approved by the organization's CIO and ISO.
- 6. Require that if a data file is downloaded to a mobile device or desktop computer from another computer system, the specifications for information integrity and cybersecurity, which have been established for the original data file, must be applied in the new environment.
- 7. Require encryption, or equally effective measures, for all personal, sensitive or confidential information that is stored on portable electronic storage media and on portable computing devices.

Section 5.2 USG Appropriate Usage Standard

To enable delivery of reliable, efficient and effective technology services, the University System of Georgia (USG) requires all users, including institutions, employees, students, contractors, guests, vendors and any other authorized person or organization ("users"), of all USG Information Technology (IT) resources and services to conduct themselves responsibly. IT resources and services include but are not limited to hardware, software, networks, data, the internet when accessed through USG resources, and communication systems, whether owned, leased, or otherwise provided by USG organizations ("resources"). Users of USG IT resources must respect the public trust that provides the resources; comply with federal, state and local laws; comply with USG policies, standards and directives; respect the rights and privacy of others; and respect the integrity of USG facilities and controls. This standard applies to all users of USG IT resources.

5.2.1 Requirements

Appropriate use of USG IT resources is an enterprise-wide undertaking necessitating that all users promote responsible behavior and create safeguards against abuse of USG IT resources. Therefore, all users are obliged to abide by the following general standards:

- 1. Use only resources for which authorization is granted. For example, it is a violation to:
 - a) Prevent others from accessing a service to which they are authorized;
 - b) Use resources for which the user is not specifically authorized;
 - c) Use someone else's user account and password;
 - d) Share user accounts and passwords with someone else;
 - e) Use privileged access for purposes other than official duties; and
 - f) Use unauthorized third-party software or information services to store, access or process USG information.
- 2. Use resources only for their intended purposes. For example, it is a violation to:
 - a) Use resources for advertising or commercial purposes other than for official USG business;
 - b) Misuse software to conceal anyone's identity or attempt to circumvent security safeguards;

- c) Interfere with resources that impair or inhibit the work of other users;
 - d) Create or forward threats, hoaxes, chain letters or forged email, except to report them; and
 - e) Intercept or monitor any network communications not intended for you without permission or in support of official duties.
3. Respect the privacy and personal rights of others. For example, it is a violation to:
- a) Disclose information about faculty, staff and students in violation of federal, state, local law, directives or USG guidelines;
 - b) Access or attempt to access USG resources or other user accounts or credentials without authorization;
 - c) Monitor or tap data communications or traffic on USG IT resources without express permission;
 - d) Access or copy communications, data or files of other users without permission; and
 - e) Transmit, disseminate, sell, store or host material on USG resources that is unlawful, libelous, defamatory, obscene, pornographic, harassing, threatening, abusive or invasive of privacy rights.
4. Protect access, integrity and confidentiality of USG resources. For example, it is a violation to:
- a) Release malicious software that damages or harms any USG resources, including systems or networks;
 - b) Attempt to deliberately degrade performance or deny services of USG IT systems;
 - c) Corrupt, misuse, alter or destroy information without authorization;
 - d) Purposely seek or exploit security flaws to gain system or data access; and
 - e) Store protected or confidential information in unintended or unprotected locations.
5. Respect intellectual property and copyrights of others. For example, it is a violation to:
- a) Use unsupported or expired software in violation of USG guidelines;
 - b) Download, use or distribute copyrighted materials without permission;
 - c) Download, use or distribute pirated software, music, videos or games; and
 - d) Make or use more copies of licensed software than permitted.

5.2.2 Mobile Workforce Requirements

Although USG IT service providers are charged with preserving the integrity, confidentiality, availability and security of USG managed data and information resources, security may be compromised through actions beyond any user's control. Among these, personally owned or so-called bring-your-own-devices (BYODs) used by any user presents a special risk to USG resources because device owners install and configure software applications, security settings and perform their own maintenance and may share the device with others. If BYODs are permitted to access USG IT resources, the user authorizing such access must create and publicize appropriate policies and guidelines delineating responsibilities to ensure appropriate security.

Responsibilities for any USG user permitting BYODs should include, at a minimum:

- a) Determining the types of devices and software versions that are permitted;
- b) Defining the minimum level of access controls, which may include device registration;
- c) Detailing which non-USG BYOD applications are supported;
- d) Detailing the types of data protection and security required for permitted devices;
- e) Disclosing the type of action taken on BYODs when employees are terminated or separated;
- f) Describing what organizational information is permitted on personal devices;

- g) Providing a disclaimer of liability for personal data loss; and
- h) Notifying users of disclosure requirements under the Georgia Open Records Act.

Responsibilities for users of BYODs are, at a minimum:

- a) Safeguarding USG account credentials and using multi-factor authentication where possible;
- b) Use of a Virtual Private Network (VPN) connection, personal firewall and antivirus protection;
- c) Backing up USG data regularly and storing all USG data in USG-managed infrastructure;
- d) Avoiding the use of unauthorized third-party software or storage facilities for USG information;
- e) Installing security patches in a timely manner; and
- f) Promptly reporting USG data loss from BYODs, misuse or violation of this standard.
- g) Complying with applicable policies and laws when using personally owned devices.

5.2.3 Enforcement

Every user has an obligation to report suspected violations of this standard using the USG institution's incident reporting procedures or to the USG Shared Service Center. Furthermore, any user engaging in unethical and/or inappropriate practices that violate USG standards is subject to disciplinary proceedings that may include suspension of system privileges, expulsion, termination and/or legal action as appropriate. If a user is suspected of violating USG standards or policy, any right to privacy may be superseded by USG's requirement to protect the integrity of IT resources, the rights of all users, and state assets. The USG reserves the right to examine material stored on or is transmitted through IT resources to maintain appropriate standards of conduct and duty of care.

Section 5.3 Cybersecurity Incident Management

The number of cybersecurity incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing mature cybersecurity policies, limiting access to networks and computers, improving user security awareness, and early detection and mitigation of cybersecurity risks are some of the preventative actions that can be taken to reduce the risk, frequency and the cost of cybersecurity incidents. However, not all incidents can be prevented. Therefore, a cybersecurity incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing and networking services.

Proper cybersecurity incident management includes the formulation and adoption of a written cybersecurity incident management plan, providing for the timely assembly of appropriate staff that can develop a response to, appropriate reporting about, and successful recovery from a variety of incidents. Furthermore, cybersecurity incident management includes the application of lessons learned from incidents together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences in the future.

5.3.1 Cybersecurity Incident Response Plan Requirements

USG organizations shall establish and document an internal cybersecurity incident management capability, providing for prevention, monitoring, detection, containment, response, recovery, reporting and escalation, appropriate to the level of risk and threats to the USG organization. Concerning organizational incident response plans, USG Cybersecurity modeled NIST SP800-53 (Rev4) IR-8, which consists of thirteen requirements. This aligns with the federal requirement to implement National Institute of Standards and Technology (NIST) and Gramm-Leach-Bliley Act (GLBA) in support of the Federal Student Aid compliance efforts. In accordance with Board of Regents Policy Section 10.4, USG

organizations must submit a copy of their cybersecurity incident response plans to USG Cybersecurity. USG Cybersecurity shall evaluate USG organizational submissions against the NIST model and provide guidance concerning any findings affecting the maturity of the submitted plans.

Requirements

USG organizations shall:

- a. Develop a Cybersecurity Incident Response Plan (IRP) that:
 1. Provides the organization with a roadmap for implementing its cybersecurity incident response capability;
 2. Describes the structure and organization of the cybersecurity incident response capability;
 3. Provides a high-level approach for how the cybersecurity incident response capability fits into the overall organization;
 4. Meets the unique requirements of the organization, which relate to mission, size, structure and functions (e.g., Cybersecurity Playbooks – Data Privacy, DDOS, PII Breach, Ransomware and other relevant topics);
 5. Defines reportable cybersecurity incidents, which includes how...
 - i. Notification alerts are investigated;
 - ii. Impacts are understood;
 - iii. Incidents are categorized;
 - iv. Incidents are contained; and,
 - v. Incidents are mitigated.
 6. Provides metrics (incident alert thresholds) for measuring the cybersecurity incident response capability within the organization;
 7. Defines the resources and management support needed to effectively maintain and mature a cybersecurity incident response capability; and
 8. Reviews and approves plan by organization-defined personnel or roles.
- b. Distribute copies of the cybersecurity IRP to organization-defined cybersecurity incident response personnel (identified by name and/or by role) and organizational elements;
- c. Review cybersecurity IRP following organization-defined frequency;
- d. Update the cybersecurity IRP to address system/organizational changes or problems encountered during plan implementation, execution or testing;
- e. Communicate cybersecurity IRP changes to organization-defined cybersecurity incident response personnel (identified by name and/or by role) and organizational elements;
- f. Protect the cybersecurity IRP from unauthorized disclosure and modification; and,
- g. Response plans are tested following organization-defined frequency.

5.3.2 Cybersecurity Incident Reporting Requirements

USG organizations must establish a cybersecurity incident response plan to respond to and manage adverse activities or actions that threaten the successful conduct of teaching, research, service, and operations in the USG.

Requirements

- a. All incident response reporting and escalation procedures must be formally documented and approved by USG Cybersecurity.
 1. Cybersecurity events refer to any questionable or suspicious activity that could threaten the security of sensitive data and/or our information systems infrastructure. These events may or may not have criminal implications. Examples include reconnaissance activity or human error.
 2. Cybersecurity incidents are violations (or imminent threats of violation) of cybersecurity policies, acceptable use policies, standard cybersecurity practices, and federal and state cybersecurity and privacy legislation. Examples include an information system being “hacked” or the loss of a thumb drive containing sensitive data.
- b. USG organizations must train employees on how to recognize and report cybersecurity incidents in accordance with the reporting and escalation procedures.
- c. USG organizations must have a designated and documented incident management point of contact.
- d. A timely response is critical. USG organizations must report all cybersecurity incidents or events of interest affecting systems or data for any of the security objectives of confidentiality, integrity or availability to USG Cybersecurity through the Enterprise Service Desk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3697 (toll free within Georgia).
 1. Timely Response is defined by the type of data or information breached and the regulation governing the breach notification. For example, some regulations state within 24 hours of discovery, other regulations state most expediate time possible, or without reasonable delay.
 2. All cybersecurity incidents affecting the operation of mission-critical systems and categorized as “High” shall be reported to USG Cybersecurity within one hour of identification. In accordance with the Georgia Cybersecurity Board memo dated 09/08/2020, USG Cybersecurity has the responsibility to notify the governor’s office or delegated authorities.
 3. Additionally, all cybersecurity incidents that requires reporting to any federal agency must be reported to USG Cybersecurity within one hour of identification, USG Cybersecurity has two hours upon identification to report to the Director of Emergency Management and Homeland Security in accordance with O.C.G.A. 38-3-22 (amended 2021).
 - a. The types of incidents USG organizations must report to USG Cybersecurity include “type of cyber-attack, data breach, or use of malware” if these criteria are met that...
 - i. Creates a life-safety event, or

- ii. Substantially impacts the security of data and information systems, or
 - iii. Affects critical systems, equipment, or service delivery.
- b. No USG organization is exempt from this reporting structure. O.C.G.A. 38-3-22.2 (amended 2021) (d) also states, “Any reports or records pursuant to this Code section shall not be subject to public inspection or disclosure under Article 4 of Chapter 18, of Title 50.” ²
- e. In addition, as part of the post-incident activity, an incident follow-up report must be submitted to the USG Cybersecurity that includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed at preventing or mitigating the risk of similar occurrences in the future.

5.3.3 Cybersecurity Events/Incidents Involving Personal Information

In addition to the above listed requirements, any USG organizations that collect, use, or maintain records containing personal information shall establish and maintain procedures in its cybersecurity incident management program for ensuring that any breach of cybersecurity or data privacy involving personal information, regardless of its medium (e.g., paper, electronic, verbal) shall immediately trigger the cybersecurity incident response process. Plans and procedures must be documented and address, at a minimum, the following:

- a. Identification of Roles and Responsibilities (reference USG Incident Response Plan template available within the USG Cybersecurity SharePoint site). Plans shall identify the roles responsible for responding to a breach of personal information.
 - 1. Reference Section 5.3.2 Cybersecurity Incident Reporting Requirements.
 - 2. Cyber Liability Insurance Decision Trigger
 - i. 1st Criteria: EXPOSURE - any protected personal identifiable information exposed (unencrypted) to unauthorized access.
 - ii. 2nd Criteria: SCOPE - breach of systems, products, or services needing forensic support, size of attack, potential civil/criminal prosecution.
- b. Protocol for Internal Reporting. Procedures shall outline the method, manner, and progression of internal reporting to ensure that executive management is informed about breaches involving personal information.
- c. Decision Making Criteria and Protocol for Notifying Individuals. Procedures shall include documentation of the methods and manner for determining when and how a notification is to be made. The procedures shall be consistent and comply with USG policies and applicable state and federal laws. At a minimum, these procedures will address the following elements:
 - Whether the notification is required by law;
 - Whether the notification is required by USG or state or federal policy;
 - Timeliness of notification;
 - Source of notice;
 - Content of notice;
 - Approval of notice prior to release;

² <https://gov.georgia.gov/document/2021-signed-legislation/hb-156/download>

- Method(s) of notification;
- Preparation for follow-on inquiries;
- Other actions that can be taken to mitigate harm to individuals; and,
- Other situations when notification should be considered.

5.3.4 Cybersecurity Events/Incidents Involving Suppliers

A supplier (third-party) data or information exposure affecting members of the USG community resulting or has the potential for resulting in a press release characterizes the type of incident that is to be reported to USG Cybersecurity... if for no other reason but to inform the Board of Regents and Executive Leadership that the USG was not breached but that a third party was breached exposing the protected data of members of the USG community.

USG organizations shall file an incident ticket with USG Cybersecurity regardless of whether a current contract with the supplier exists. If an organization has members of its community conducting business with a supplier and that supplier is associated with the organization and that supplier exposes data, submit an informational ticket to USG Cybersecurity of the supplier's exposure of your community's data.

USG organizations shall follow up with the supplier to ensure they provide notification and mitigation concerning the exposure.

Section 5.4 USG Information Asset Management and Protection

Information assets can be defined as:

1. All categories of automated information, including, but not limited to, records, files and data bases; and,
2. Information technology facilities, equipment (including endpoints, personal computer systems) and software owned or leased by a USG organization.

5.4.1 USG Information Asset Management Requirements

Asset inventory is required by state asset management procedures and is the method by which the USG maintains accountability of the systems, products or services, such as physical computing devices and software purchased with state funds.

Requirements

Each USG organization shall maintain perpetual and up-to-date accountability of all hardware and software (including licenses) acquired with federal or state funds. This also includes all supplier managed systems, products and services that accesses, stores processes, and transmits USG information assets. In the case of shared resource situations among two or more USG organizations, the hosting organization shall be responsible for this accountability. All assets shall be recorded in compliance with all applicable state or USG asset management policies and the Official Code of Georgia Annotated section 50-16-160 et. seq. Asset management shall include procedures for accountability throughout the asset's life cycle from acquisition to decommission, transfer of ownership, surplus and/or equipment refresh/upgrades.

5.4.2 USG Information Asset Protection Requirements

USG organizations must provide for the integrity and security of their information assets by identifying all information systems, products, or services for which that USG organization has ownership

responsibility, and ensuring that responsibility for each information system, automated file, or database is defined with respect to:

1. Owners of the information system;
2. Owners of the information within USG organizations;
3. Trustees and stewards of the information;
4. Users of the information;
5. Classification of information to ensure that each automated file or database is identified as to its information class in accordance with policies and standards;
6. The data processing environment is identified (e.g., geographic location, on-premises, cloud, or third party managed). Service Providers ("Suppliers") will provide services to USG solely from data centers physically located in the United States;
7. Storage of USG data at rest will be located/stored solely in data centers in the United States; Suppliers will process USG data outside of the United States data centers only to provide services to USG end users located outside of the United States. The term "data center" herein is defined as all supplier facilities and those used by Supplier's contractors in which USG data is processed or stored;
8. Identified assets are scanned for vulnerabilities, which are documented and mitigated or remediated; and,
9. Systems, products, services, and associated data are formally managed throughout removal, transitions, and disposition.

Note: The definitions of Owners, Stewards, Trustees, and Users are covered in the BOR *BPM*, Section 12: Data Governance and Management.

Section 5.5 Risk Management

Cybersecurity risk management is a strategic business discipline that supports the achievement of an organization's objectives and goals by addressing the full spectrum of its risks and managing the combined impact of those risks. Risk management is an aggregation of three processes – risk assessment, risk mitigation, and controls evaluation and measurement. Risk management helps an organization ensure integration of strategic and operational planning processes. Managing risk safeguards the organization's mission and goals and requires an ongoing evaluation and assessment of operations and processes. USG information assets (e.g., data processing capabilities, information technology infrastructure and data) are an essential resource and asset. For many organizations, program operations would effectively cease in the absence of key computer systems, products, or services. In some cases, public health and safety would be immediately jeopardized by the failure or disruption of a system. Furthermore, the unauthorized modification, deletion or disclosure of information included in institution files and databases can compromise the integrity of USG programs, violate individual right to privacy, and constitute a criminal act.

5.5.1 Risk Assessment and Analysis Requirements

USG organizations must ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction, or disclosure and to confirm the physical security of these resources. USG organizations shall also ensure that users, contractors, and third parties having

access to state or USG computerized information resources are informed of and abide by this standard and the USG organizations' cybersecurity plan and are informed of applicable local, state, and federal policies, laws, regulations, and/or codes related to computerized information resources. USG organizations must establish a risk management process to identify, assess, and respond to the risks associated with its information assets.

Risk Assessment: Concerning organizational risk management plans, USG Cybersecurity modeled NIST SP800-53 (Rev4) RA-3, which consists of five requirements. USG organizations shall...

1. Assess risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
 - a. USG organizations understand the cybersecurity (including supplier) and data privacy risks to individuals, products, and systems and how they may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial, reputation, workforce and culture.) Event data (logs) shall be collected and correlated from sources and sensors.
2. Document risk assessment results in an organization-defined document;
 - a. Policies, processes and procedures incorporate lessons learned from problematic data actions and/or safeguard failures or weaknesses.
 - b. USG Cybersecurity has provided a cybersecurity risk template spreadsheet to manage and track risks and mitigation efforts.
3. Review risk assessment results following an organization-defined frequency (remembering to consider supplier and data privacy risks);
 - a. Supplier relationships are identified. Suppliers include contracted systems, products or services, third parties, and external vendors to list a few.
 - b. Potential problematic data actions are identified. A problematic data action is defined as a data action that could cause an adverse effect for individuals (e.g., unauthorized access/exposure), which is the focus concerning data privacy.
 - c. Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources.
 - d. Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
4. Disseminate risk assessment results to organization-defined leadership; and
5. Update the risk assessment following an organization-defined frequency (e.g., annually, biannually, etc.) or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the cybersecurity state of the system.

Risk Analysis: Following risk assessment, risk analysis is performed commensurate to the level of sensitivity of the information resources identified, in which IT-related assets (e.g., information, people – both internal and external to the organization – software, hardware, facilities, etc.) are identified and which of those assets are determined to be most critical to protect, the threats to which they are

subject must be identified and evaluated. USG organizations must ensure the policies, processes, and procedures for ongoing review of the organization's cybersecurity, and data privacy posture are understood and informs the management of assessed and analyzed risk.

Risk Register: The risk management tool used to record the risk assessment is a risk register. Risks are identified to include nature of risk, level of risk, impact and frequency of risk, reference the owner of the risk, and the mitigating measures in place to respond to the risk of the data ecosystems, products and services. For a given IT asset, an estimate should be made of the largest potential business impact, based on failures of confidentiality, integrity, and availability. The relative business impact of these three types of failure events should then be estimated as high, medium, or low. For example, if a system is estimated as having a low requirement for confidentiality, a medium requirement for data integrity, and a high requirement for service availability, then that IT asset is treated as having a high requirement for attention.

5.5.2 Defining Risk Tolerance

Senior leadership at each USG organization shall decide when a residual level of risk may be acceptable. The choices available to senior leadership includes the following activities pertaining to each of the identified risks to determine an appropriate risk response:

1. Mitigate the risk (by choosing to engage in an action with safeguards);
2. Accept the risk (by choosing to engage in an action without safeguards);
3. Avoid the risk (by choosing not to engage in an action); or,
4. Transfer the risk (by choosing to move the risk to another party).

5.5.3 USG Organizations Risk Management Programs

The practice of risk management within a USG organization must be based upon architecture, contracted external supplier relationship and the results of the organization's risk analysis process. Supplier (e.g., contracted, third-party, external vendor...) risk management addresses three components beginning with supplier risk assessment process; the second component concerns contracts; and the third component concerns contract/supplier evaluation. All three of these components are addressed within the *Business Procedures Management*, Section 3.4 Contracts.³ Based on the impact analysis and the risk assessment, the organization should determine what types of safeguards are appropriate to address their defined risks. In this manner, the safeguards deployed reflect the true importance of the investment in the information resources used to accomplish the organization's mission.

A risk management plan must then be developed documenting the actions and safeguards (or countermeasures) that can be taken to reduce the identified risks based on available resources. While it is not required that this plan be on file with USG Cybersecurity, it must be made available upon request. A focus on the USG and organization missions is vital. The IT organization cannot, and is not expected to, mitigate every risk but must prioritize based on the threat to the mission and available resources. Obtaining resources for risk management is subject to the same technical, programmatic, and budgetary justification and review processes required for any information technology program. The risk management practices implemented by each USG organization will vary depending upon the nature of the organization's information assets.

³ https://www.usg.edu/business_procedures_manual/ (*Under Review*)

5.5.4 USG Cybersecurity Risk Management Process

Federal and state information technology regulations require USG information resources to undergo a cybersecurity risk management process to identify the risks associated with their operation and to take steps to reduce and maintain that risk to an acceptable level. Risk management is integral to the development and operation of information resources.

Process

Cybersecurity risk management planners must communicate and collaborate with the USG organization's enterprise risk management (ERM) coordinator, at least annually. Cybersecurity risk management practices implemented will vary depending upon the nature of the USG organization's information assets. Practices that must be included in each organization's risk management program are:

1. Discover and inventory endpoints and data;
2. Categorize the information system (impact/criticality/sensitivity);
3. Select and tailor baseline (minimum) security safeguards;
4. Supplement the security safeguards where required based on risk assessment;
5. Document security safeguards in the system security plan;
6. Implement the security safeguards in the information system;
7. Assess the security controls for effectiveness;
8. Authorize information system operation based on mission risk; and,
9. Continuously monitor security safeguards for potential cybersecurity events that includes:
 - a. Detecting network-based activity;
 - b. Detecting environment-based activity;
 - c. Detecting personnel-based activity (insider); and,
 - d. Detecting malicious code to include unauthorized mobile code.

Section 5.6 USG Information System Categorization

Data is a critical asset of the USG. USG organizations have a responsibility to protect the confidentiality, integrity, and availability of the information and information systems assets utilized. However, to adequately protect the data, there must be an understanding of what to protect, why protect it and how to protect it. The security objective is to maintain the confidentiality, integrity, and availability of all information and information systems, products or services. Security categorization is the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organization operations, assets, or individuals and the USG itself to include all USG contracted suppliers that accesses, stores, processes and transmits data and information assets on behalf of the USG. Confidentiality, integrity and availability are defined as:

1. Confidentiality - "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..." [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.
2. Integrity - "Guarding against improper information modification or destruction and includes ensuring information non - repudiation and authenticity..." [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.

3. Availability - “Ensuring timely and reliable access to and use of information...” [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to, or use of, information or an information system.

5.6.1 Purpose

Security categories are based on the potential impact to an organization or supplier operation on behalf of the USG should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals.

5.6.2 Requirements

Data Owners shall inventory, provide data flow diagrams and assign a security category to the information systems for which they hold responsibility. The security category assigned shall conform to *FIPS Publication 199, Standards for Security Categorization for Federal Information Systems*, which addresses developing standards for categorizing information and information systems according to the potential impact on organizations should there be a breach in security.

Specifically:

1. The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.
2. The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.
3. The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.

Security categorization information is shown in the “Nine Box” from FIPS Publication 199, as shown below.

Table 5.3: NIST “Nine Box” Security Categorization

	Low	Moderate	High
Confidentiality	The loss of confidentiality could be expected to have a <u>limited</u> adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a <u>serious</u> adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a severe or <u>catastrophic</u> adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a limited adverse effect on organizational	The loss of availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

	operations, organizational assets, or individuals.		
--	--	--	--

The generalized format for expressing the security category (SC) of an information system is:

- SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}, where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

The security categorization process is carried out by the information system owner and information owner/ steward in cooperation and collaboration with appropriate organizational officials (i.e., senior leaders with mission/business function and/or information security officer/risk management responsibilities). The security categorization process is conducted as an organization-wide activity taking into consideration the enterprise architecture, cybersecurity architecture and external suppliers that access, store, process and/or transmit USG data and information assets. This helps to ensure that individual information systems are categorized based on the mission and business objectives of the organization. Additionally, systems dependencies as illustrated within data flow diagrams can be mapped and inventoried to be used in determining mission criticality. The results of the security categorization process influence the selection of appropriate security controls for the information system and, where applicable, the minimum assurance requirements for that system. Security categorization information must be documented in the system identification section of the security plan or included as an attachment to the plan.

“Mission-Critical System” designation uses the output of the categorization process. A mission-critical system is a system whose failure or malfunction will result in not achieving organizational goals and objectives. Criteria are a) contains confidential or sensitive data (i.e. personally identifiable information (PII) and other regulated information), or b) serves a critical and necessary function for daily operations, or c) a combination of both protected data and critical function.

Section 5.7 USG Classification of Information

The USG’s records (paper or electronic, including automated files and databases) are essential public resources that must be given appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion.

5.7.1 Classification Structure

USG organizations must classify records using the following classification structure:

1. *Unrestricted/Public Information* is information maintained by a USG organization that is not exempt from disclosure under the provisions of an open records act or other applicable state or federal laws.
2. *Sensitive Information* is information maintained by a USG organization that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher-than-normal assurance of accuracy and completeness. Thus, the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of USG financial transactions, student records, and/or regulatory actions.

3. *Confidential Information* is information maintained by a USG organization that is exempt from disclosure under the provisions of an open records act⁴ or other applicable state or federal laws.

5.7.2 Defining Personal Information

In addition, Personal Information may occur in unrestricted/public, sensitive and/or confidential information. Personal Information identifies or describes an entity by name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to name, address, telephone number, Social Security number (SSN), date of birth, government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer Internet Protocol address or routing code and credit card number, or other credit card information. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. Personal information includes, but is not limited to:

1. Protected Health Information (PHI) - individually identifiable health information created, transmitted, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. Federal regulations require state entities that are health plans, health care clearinghouses, health care providers or entities declared as "business associates" conducting electronic transactions ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure.
2. Personally Identifiable Information (PII) - any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the institution. Some PII is not confidential, such as the PII on a business card, while other PII is considered Sensitive Personally Identifiable Information (Sensitive PII). If lost, compromised, or disclosed without authorization, Sensitive PII could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.⁵

The designated owner⁶ of a record is responsible for making the determination as to whether that record should be classified as public, sensitive, or confidential. The owner of the record is responsible for defining special security precautions that must be followed to ensure the integrity, security, and appropriate level of confidentiality of the information. Records containing sensitive and/or personal information require special precautions to prevent inappropriate disclosure. When confidential, sensitive, or personal information is contained in public records, procedures must be used to protect it from inappropriate disclosure. Such procedures include the removal, redaction, or otherwise masking of the confidential, sensitive, or personal portions of the information before a public record is released or disclosed. While the need for the USG organizations to protect data from inappropriate disclosure is important, so is the need for the USG organization to take necessary action to preserve the integrity of

⁴ Georgia's open records act is located at: <http://law.ga.gov/law>.

⁵ O.C.G.A. 10-1-910

⁶ The definition of Owner is covered in the Business Procedures Manual Section 12, Data Governance and Management.

the data. USG organizations must develop and implement procedures for access, handling, and maintenance of personal and sensitive information. Information classification must be part of the risk management program, as detailed in Section 5.5.

Section 5.8 Endpoint Security

5.8.1 Purpose

This section provides the components, features and operational sequence for endpoint security and system management. All USG organizations must implement endpoint security by deploying the components and features listed below by the dates listed in the implementation/compliance subsection. Compliance will be formally reported and verified by the biannual USG *CPR* and USG Internal Audit and Compliance.

5.8.2 Discovery and Inventory

Data processing by systems, products, or services is understood and informs the organization of cybersecurity and data privacy risks. Endpoint discovery is the process of collecting and listing assets. Discovering state-owned assets is a fundamental step in the defense and protection of USG assets, permitting a real-time inventory and system categorization. USG organizations must employ a comprehensive real-time endpoint discovery process that can detect and discover all endpoint devices on the USG organizations' network. An up-to-date inventory of all state-owned endpoint devices must be developed, maintained and reported upon request. At a minimum, the inventory must include device name, categorization, MAC address and location. Beyond the state-owned assets, owners or managers (e.g., the organization or contracted third parties) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.

5.8.3 Anti-virus, Anti-malware, Anti-spyware Controls

Preventive or detective controls are activities that prevent or detect threats or vulnerabilities to mitigate risks. Anti-virus, anti-malware and anti-spyware protect and prevent known and emerging computer viruses, malicious programs and unwanted software applications on the endpoint. All endpoint devices must have installed and activated anti-virus, anti-malware and anti-spyware protection software. Anti-virus is a mandatory foundational control for protecting state-owned assets against certain attack vectors. Where possible, anti-virus software must be installed and configured for automatic updates on desktops, portables and mobile assets. Anti-malware software is designed to prevent, detect and remediate malicious programming on endpoint systems. Where possible, anti-malware software must be installed and configured for automatic updates on desktops, portables and mobile assets. Anti-spyware software is designed to prevent, detect and remediate spyware programs on endpoint systems. Where possible, anti-spyware software must be installed and configured for automatic updates on desktops, portables and mobile assets.

5.8.4 Operating System (OS)/Application Patch Management

To ensure the security of our network and protect USG data, all endpoint assets must be securely maintained, and critical security patches must be applied consistent with an assessment of risk. Desktop and mobile assets must have activated and operating patch management solutions.

5.8.5 Maintenance

Maintenance and repairs of information system components is performed consistent with procedures. USG organizations must show maintenance and repair of organizational assets is performed and logged

in a timely manner, with approved and controlled tools. USG organizations shall maintain and repair organizational assets, record the maintenance and repair, and do so utilizing pre-approved and vetted tools. Additionally, if remote maintenance is required, it must be approved, logging enabled and performed in a manner that prevents unauthorized access.

Section 5.9 Cybersecurity Awareness, Training and Education

Given the increased use of IT and Internet-based services, the USG has a compelling need to ensure confidentiality, integrity and availability of those systems, products or services as well as adequate protection from known and anticipated threats. As noted in Section 5.2.2 of the *USG IT Handbook*, USG organizations are responsible for the designation of officials to fulfill key cybersecurity functions and report on status of compliance with cybersecurity policy, standards and procedures.

5.9.1 Roles and Responsibilities

While it is important to understand the policies, standards and guidelines (PSG) that USG organizations develop and implement, it is crucial that faculty, staff, students and third-party affiliates understand who has responsibility for cybersecurity and data privacy defense.

Organization President or Chief Executive

The Chancellor, organization president or chief executive and senior leadership are responsible for ensuring that appropriate and auditable cybersecurity controls are in place to include awareness, training and education as stated within *Board of Regents Policy 10.4*.

Information Security Officer (ISO)

The ISO shall provide leadership in cybersecurity awareness, training and education as well as work with the academic, administrative and information technology leadership to:

1. Establish overall strategy for cybersecurity awareness, training and education.
2. Understand program maturity and compliance.
3. Provide evidence semiannually using the Cybersecurity Program Review (CPR) that all users accessing information or information systems, products or services are trained in their cybersecurity responsibilities.
4. Identify who within the organization has the data privacy role and coordinate the implementation of cybersecurity data privacy support responsibilities.

Users

Users are the largest audience and most important group to help reduce unintentional errors and vulnerabilities. Users requiring access to information and information systems, products or services must:

1. Understand and comply with USG organization's cybersecurity policies and procedures.
2. Be trained in the acceptable use of the systems, products or services to which they have access.
3. Work with management to meet training needs.
4. Be aware of actions to better protect USG organization's information and information systems, products or services. These include, but are not limited to password usage, data management, antivirus protection, incident reporting and actions to avoid social engineering attacks.

Third Party

Third parties (e.g., services providers, customers, partners) have been identified and they understand their roles and responsibilities concerning awareness training.

5.9.2 Cybersecurity Awareness, Training and Education Requirements

USG organizations cannot protect confidentiality, integrity and availability of information and information systems, products or services without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them.

Learning Objectives

USG organizations shall provide cybersecurity awareness training to users that access information or information systems, products or services. Topics covered must include:

- Cybersecurity policy and guidelines and the need for cybersecurity;
- Data governance and management as well as roles and responsibilities;
- Importance of personal cybersecurity; and,
- Threats to cybersecurity and incident reporting.

Awareness training shall be conducted biannually, attendance shall be mandatory, completion shall be documented and shall provide practical and simple guidance pertaining to user roles and responsibilities. Additional role-based cybersecurity training shall be provided to IT specialists, developers, cybersecurity management and users having unique or specific cybersecurity responsibilities.

Enabling Learning Objectives:

- To know where to locate within the organization the PSGs governing cybersecurity.
- To know data governance, which data is protected and why, and one's role and responsibility.
- To know why personal cybersecurity is important.
- To know how to identify threats to the information assets and what to do to report them.

Terminal Learning Objectives:

- To raise awareness to the content's importance in reducing cybersecurity risk within the USG.
- To know the vocabulary.

Training Requirements

1. Cybersecurity policy and guidelines and the need for cybersecurity:
 - Define the location of USG's PSG's governing cybersecurity.
 - Define the location of the USG organizations' PSGs governing cybersecurity.
 - Define the location of relevant regulatory, industry and compliance legislation and standards.
 - Define data confidentiality, integrity and availability (*Reference: BPM Section 12*).
 - Define the factors contributing to the need for cybersecurity:
 - Establishing a standard of due care.
 - Elevation of threats – social engineering, mobile devices.
 - Technological growth and ubiquitous presence.

- Data integrity and cross connectivity (shared services).
 - Compliance expectations.
2. Data governance and management (*Reference: BPM Section 12*).
- Define the USG organizations' data management structure.
 - Define roles and responsibilities.
 - Data Owner, Data Trustee, Data Stewards and Data Users.
 - Define which data is protected and why.
 - Define the data classification process.
 - Define data handling procedures for protected data.
3. Importance of personal cybersecurity.
- Define personally identifiable information (PII) and why it is important to protect.
 - Raise awareness of the Appropriate Usage Policy (AUP).
 - Define the AUP's location.
 - Describe the AUP's use.
 - Describe how to protect online transactions.
 - Identify identity theft efforts and what to protect.
4. Threats to cybersecurity and incident reporting.
- Describe how to identify threats to the information assets.
 - Define threat categories:
 - Application.
 - Access control/authentication/authorization.
 - Cybercrime/social engineering/legal.
 - Data exposure/privacy.
 - Environmental.
 - Physical systems and facilities.
 - Identify the most common vectors of cybersecurity threats.
 - Describe how to report an incident.
 - USG organizations to the USG in accordance with:
 - Information Technology Handbook requirements.
 - Federal, state and industry legislative and/or regulatory requirements.
 - End users to the USG organizations.

Recommended Tools and Materials

- USG organizational learning management system (LMS).
- USG organizationally developed LMS.
- Awareness training module delivered via electronic presentation.
- Document-based awareness training module.

Section 5.10 Required Reporting

The USG has a compelling need to ensure confidentiality, integrity and availability of IT systems, products or services as well as adequate protection from known and anticipated threats. As noted in Section 5.1.2 of the *USG IT Handbook*, USG organizations are responsible for the designation of officials to fulfill key cybersecurity functions and report on status of compliance with cybersecurity policy, standards and procedures.

5.10.1 Required Reporting Activities

The following provides a summary list and schedule of required cybersecurity reporting activities with corresponding due dates. Unless otherwise noted, all reports must be submitted in electronic format to USG Cybersecurity.

Cybersecurity Officer Contact Information Update

As noted in Section 5.1.2 of the *USG IT Handbook*, the name and appropriate designee contact information must be sent to USG Cybersecurity within 10 business days of any designee change.

Cybersecurity Incident Response Plan Submission

As noted in Section 5.3.1 of the *USG IT Handbook*, a cybersecurity incident response plan must be formally documented and electronically sent and filed with USG Cybersecurity.

Cybersecurity Incident Reporting Requirement

As noted in Section 5.3.2 of the *USG IT Handbook*, a timely response is critical. USG organizations must report all cybersecurity incidents or events of interest affecting information or information systems, products, or services for any of the cybersecurity objectives of confidentiality, integrity, or availability to USG Cybersecurity through the ITS Helpdesk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3697 (toll free within Georgia). For all incidents affecting mission-critical systems and categorized as “**High**” shall be reported to USG Cybersecurity within **one hour** of identification.

Cybersecurity Incident Follow-up Reporting Requirement

As noted in Section 5.3.3 of the *USG IT Handbook*, an incident follow-up report must be submitted to USG Cybersecurity.

Cybersecurity Program Review (CPR) Submission

The Governor’s Executive Order of March 19, 2008, requires development of a composite report on the status of cybersecurity for all state agencies. The USG has chosen to align itself with this order by producing its own USG CPR. Reference **Figure 4** Required Reporting Diagram. USG Cybersecurity will complete the following CPR processes on an annual basis:

- **April:** USG Cybersecurity shall review previous CPR reports to determine if changes are required and identify areas of focus for the upcoming review period. USG Information Technology Services (ITS) senior staff and the Internal Audit and Compliance department will review proposed changes. USG Cybersecurity shall inform USG organization of any revisions to the report, changes to the CPR reporting process and the areas of focus for the upcoming review period.



Figure 4: Required Reporting Diagram (Updated)

- **May:** USG Cybersecurity releases the Spring CPR Survey to USG organizations. USG organizations have 30 days to complete the survey.
- **June:** USG Cybersecurity collects, compiles and analyzes Spring CPR Survey results.
- **November:** USG Cybersecurity releases the Fall CPR Survey to USG organizations. USG organizations have 30 days to complete the survey.
- **December:** USG Cybersecurity collects, compiles and analyzes Fall CPR Survey results.
- **January:** USG Cybersecurity shall merge the spring and fall analysis into the annual cybersecurity risk and maturity report and make available to respective USG CIOs, CISOs and USO senior staff.

Remediation and Mitigation Tracker Submission

Remediation and mitigation trackers provide a standardized method for USG organizations to represent the plan of actions and milestones to close on such tasks as Internal Audit findings, Federal Student Aid compliance, and special projects like multi-factor authentication deployment. Reference **Figure 4** Required Reporting Diagram. USG Cybersecurity will complete the following remediation/mitigation tracker processes on an annual basis:

- **February:** USG Cybersecurity requests USG organizations to update winter Remediation and Mitigation Trackers (trackers). USG organizations are permitted 31 days to complete the trackers.
- **March:** USG Cybersecurity collects, compiles and analyzes the updated winter trackers.
- **August:** USG Cybersecurity requests USG organizations to update summer trackers. USG organizations are permitted 31 days to complete the trackers.
- **September:** USG Cybersecurity collects, compiles and analyzes the updated summer trackers.
- **October:** The winter and summer analysis of the trackers are merged into the annual report(s) respective to what is being tracked (i.e., Audit, MFA FSA....), which shall be made available to respective USG CIOs, CISOs and USO senior staff.

Risk management is a broad area requiring top-level management attention and USG-wide participation. Cybersecurity policies, standards and guidelines are intended to reduce business risk throughout USG

organizations. USG organizations have the responsibility of providing cybersecurity to protect USG's data. USG organizations are required to conduct reviews of their cybersecurity programs twice annually and submit the results to USG Cybersecurity. These data will be used to prepare the annual enterprise cybersecurity risk and maturity report. Components of the CPR are as follows:

1. **Personnel: Goal(s)** – Track and quantify dedicated and trained information cybersecurity professionals designated as USG organizational cybersecurity contacts. Advance succession planning in support of Continuity of Operations Planning (COOP).
2. **Policy and Compliance: Goal(s)** – Develop a full life cycle policy development process, refreshment and retirement methodology based on current best practices.
3. **Governance and Planning: Goal(s)** – Implement oversight and develop a cybersecurity strategy or strategies. Each strategy is supported by one or more measurable objectives.
4. **Awareness Training and Education: Goal(s)** – Ensure each organization has a cybersecurity awareness program that is completed biannually by each employee and individuals who through formal, informal, contract or other types of agreements interact with USG organizational information and information systems, products or services.
5. **Cybersecurity Operations: Goals(s)** – Implement safeguards to manage daily secure operations of systems, products and services.
6. **Data Governance & Management: Goal(s)** – Establish the maturity level of the USG organization's data governance framework. Determine information technology management input into the USG organization's data governance activities.
7. **Cybersecurity Risk Management: Goal(s)** – Establish risk management planning processes for identifying, assessing and responding to risks associated with USG organizations' information assets. Verify that all IT or business processes owners have appropriately documented cybersecurity characteristics of their systems.
8. **Cybersecurity Incident Management: Goal(s)** – Track and quantify the number of USG organizations with a formal incident management capability.
9. **Contingency Planning: Goal(s)** – Ensure the USG organizations' contingency plan includes collaboration with emergency operations, planning strategies and initiatives.

5.10.2 Remediation and Mitigation Tracker

The Remediation and Mitigation Tracker tool provides a mechanism to track the managing department and point of contact (POC) information; summarizes the issues from the final audit/assessment; identifies the specific requirements to address an issue; records a scheduled completion date; and tracks the status of the remediation effort. Components of the tracker are represented in steps as follows:

1. **Issue(s).** Describe the issue(s) identified during audit engagement or annual program review, independent evaluations by internal audit or external audit, or any other work done by or on behalf of the USG. Sensitive descriptions are not necessary, but sufficient data must be provided to permit oversight and tracking. When it is necessary to provide more sensitive data, the tracker should note the sensitive nature and be protected accordingly.
2. **Rating.** Section 16.3.8 in the BOR *BPM*, Exception Ratings are assigned to each engagement observation contained in reports issued by Audit.

3. **Impact.** Enter an objective condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the control are accountable. Controls are assigned according to impact pertaining to compliance. Impact Codes indicate the consequences of a noncompliant control, which are expressed as high, medium or low, with high indicating greatest impact.
4. **POC per Issue.** Enter the role of the responsible party resolving the audit issue (e.g., CIO, network director, etc.).
5. **Resource Requirements.**
 - **People Resources Required.** Enter the estimated funding for workforce costs required to resolve the issue. This value will be added downward and across with process and technology to generate the total estimated costs.
 - **Process Resources Required.** Enter the estimated funding for process costs required to resolve the issue. This value will be added downward and across with people and technology to automatically generate the total estimated costs.
 - **Technology Resources Required.** Enter the estimated funding for technology costs required to resolve the issue. This value will be added downward and across with people and process to automatically generate the total estimated costs.
6. **Milestones.** Identify and enter the specific requirements to address an identified issue. Note that the initial milestones and completion dates should not be altered. If there are changes to any milestone, note them in Column 8, "Milestone Changes."
7. **Scheduled Completion Date.** Enter the scheduled completion date for resolving the issue. If an issue is resolved before or after the originally scheduled completion date, the actual completion date is noted in Column 9 and 10, "Status" and "Comments," respectively.
8. **Milestone Changes.** Enter changes to the completion dates and reasons for the changes.
9. **Status.** Using the pull-down tab, select one of the available options to characterize the status remediating the issue. Options available are "completed", "on track", "scheduled", "delayed" or "at risk".
10. **Comments.** Enter additional information to include details for tracking this issue. Comments may include sources of funding, obstacles and challenges to resolve the issue (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system), or reasons for scheduling changes or changes to status.

Section 5.11 Minimum Security Standards for USG Networked Devices

The following minimum cybersecurity standards are required for devices connected to the USG PeachNet™ network.

5.11.1 Software Patch Updates

Networked devices must run software for which security patches are made available in a timely fashion. They must have all currently available security patches installed. End of support software should not be utilized in production. Exceptions may be granted for patches that compromise the usability of critical applications.

5.11.2 Anti-Virus, Anti-Spam, and Anti-Phishing Software

Anti-virus, anti-spam and anti-phishing software must be running and up to date on every level of the device, including clients, file servers, mail servers and other types of networked devices.

5.11.3 Host-Based Firewall or Host-Based Intrusion Prevention Software

Host-based firewall or hosted-based intrusion prevention software for any device must be running and configured, on every level of device, including clients, file servers, mail servers and other types of networked devices. While the use of hardware firewalls is encouraged, they do not necessarily obviate the need for host-based firewalls or host-based intrusion prevention.

5.11.4 Passwords

USG electronic communications systems, products or services must identify users and authenticate and authorize access by means of user ID, passwords, or other secure authentication processes (e.g., biometrics or Smart Cards). Password length and strength must meet the Section 5.12 Password Security. In addition, shared-access systems, products, or services must enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account. All default passwords for access to network accessible devices must be modified. Passwords used by system administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device.

5.11.5 Encrypted Authentication

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the USG network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all networked devices must use only encrypted authentication mechanisms unless otherwise authorized by USG Cybersecurity. Historically insecure services such as Telnet, FTP, SNMP, POP and IMAP must be replaced by their encrypted equivalents. Encryption, or equally effective measures, is required for all personal, sensitive or confidential information, as defined in Section 5.7, that is stored on portable electronic storage media (including, but not limited to, CDs/DVDs, external/mobile storage and USB drives) and on portable computing devices (including, but not limited to laptop and notebook computers). This standard does not apply to mainframe and server tapes.

5.11.6 Physical Security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use or any number of other potentially dangerous situations. Considering this, where possible and appropriate, devices must be configured to lock and require a user to re-authenticate if left unattended for more than twenty (20) minutes.

5.11.7 Unnecessary Services

Principles of least function (disabling all unnecessary services): Service(s) not necessary for the intended purpose or operation of the device shall not be running.

5.11.8 Integrity and Segmentation

Utilizing the principle of least privilege, USG organizations shall ensure access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed

risk of unauthorized access by demonstrating that network integrity is protected and implementing network segregation, network segmentation where appropriate.

Section 5.12 Password Management

USG organizations must establish solutions that ensure necessary user access controls are in place to safeguard the actions, functions, applications, and operations of authorized users and limit or prevent the actions of unauthorized users. This is achieved by implementing digital identities, which are the amalgamation of usernames, passwords, and authentication devices, that when combined and presented to an information system, product, or service produces a non-repudiated representation of the subject for which authentication is requested. Digital identities therefore are a one-to-one mapping of users to access. The objective is to protect the confidentiality, integrity, and availability of USG's data and information assets. The guiding principles are:

1. Authorized users will have access to the resources needed to accomplish their duties. Examples to achieve the desired purpose are:
 - a. Apply the principle of least privilege (e.g., removing local user administrative privilege to the general population), and
 - b. Implement resource categorization following *IT Handbook, Section 5.6 USG Information System Categorization*.
2. Access controls shall balance cybersecurity objectives and USG mission needs.

To achieve these principles, an authentication standard must be implemented, managed, logged, and monitored.

5.12.1 USG Password Authentication Standard

All users and their activity on IT systems, products, or services should be uniquely identifiable. User identification shall be enabled through digital identities' authentication mechanisms. User access rights to all systems and data must be in line with defined and documented business needs, and job requirements must be attached to user identification following *IT Handbook, Section 3.1 Information System User Account Management*. User identification and access rights should be maintained in a central repository.

USG organizations should deploy cost-effective technical and procedural measures to establish user identification, implement authentication, and enforce access rights. For example, multi-factor authentication (MFA) is an authentication method in which the user is granted access to an information resource only after presenting two or more correct elements to an authenticator (reference *IT Handbook, Section 3.1.2 Managing Multifactor Authentication*). These measures should be reviewed periodically and kept current. This section establishes a standard for digital identities that includes composition and protection requirements.

Composition Requirements

Access to all USG information systems, products, or services used to process, store, or transfer data with a security categorization of MODERATE or higher, as defined in *IT Handbook, Section 5.6.2*, shall require the use of a digital identity that contains strong passwords or other strong authentication mechanisms. Strong passwords shall be constructed with the following characteristics:

1. Be at least ten characters in length.

2. Must contain characters from at least two of the following four types of characters:
 - a. English upper case (A-Z).
 - b. English lower case (a-z).
 - c. Numerals (0-9).
 - d. Non-alphanumeric special characters (\$, %, ^, ...).
3. Must not contain easily accessible or guessable personal information about the user or user's family, such as names, birthdays, pets' names, addresses, etc.
4. Must be verified by USG organizations against a list that contains passwords known to be commonly used, expected, or compromised; and if a known or compromised password is chosen, the user is prompted to select a new password.

Protection Requirements

A password shall be treated as confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators, and helpdesk personnel. The non-sharing of credentials is an essential practice for ascribing system activity to users or processes.

1. Users shall not write and store passwords in clear text anywhere in their office or publicly.
2. Passwords shall not be stored in a file on any computer system, including smart devices, without encryption.
3. Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.
4. Temporary or "first use" passwords (e.g., new accounts or guests) must be changed the first time the authorized user accesses the system and have a limited life of inactivity before being disabled.
5. If an account or password is suspected of being compromised, the incident must be reported in accordance with organization-defined incident response procedures.
6. User accounts that have system or administrative privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.
7. Password history must be enabled and configured to disallow the reuse of the same password for a set length of change cycles greater than four (4) times and with the same password that has been used in the past four (4) changes. Password change frequencies must be configured to limit repeated successive password changes.
8. Account lockout, or other rate-limiting mechanism, must be enabled to lock or disable the account after five unsuccessful or failed login attempts. Temporary lockouts are permitted, provided the lockout period is longer than ten minutes.
9. When single-sign-on is implemented, MFA must also be implemented.
10. If MFA is enabled, passwords must be changed every 365 days or at any time evidence suggests the current credentials are or were potentially compromised.
11. If MFA is **not** enabled (e.g., legacy systems), passwords must be changed according to the following schedule.
 - a. Administrator-level passwords shall be changed every ninety (90) days.
 - b. User-level passwords shall be changed every one-hundred-eighty (180) days.

- c. System-level (system-to-system or non-interactive services account) passwords shall be changed after a significant event (i.e., administrator departure, suspicion, or actual compromise event.)

Enforcement

USG organizations are responsible for developing internal procedures to facilitate compliance with these USG security policies and standards. Violations of this standard could result in serious cybersecurity incidents involving protected state, federal, or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution. Reference *Human Resources Administrative Practice Manual* for actions taken when considering disciplinary actions.

Section 5.13 Domain Name System Management

Guidelines for interpretation and administration of domain name security are provided in Domain Name System (DNS) Management.

Purpose

The primary security goals for DNS are data integrity and source authentication. Both are needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit.

Background

If DNS data are not properly managed, attackers can gain information that can be used to compromise other services. For example:

1. Foot-printing and unrestricted zone transfers.
2. Denial-of-service are schemes attackers use to deny availability to services.
3. Data modification and redirection.

Scope

This standard covers internal and external DNS architecture.

5.13.1 DNS Security

Roles and responsibilities of staff managing and securing the DNS architecture must be documented. USG organizations shall determine system categorization in accordance with USG *IT Handbook*, Section 5.6 and apply appropriate administrative and technical controls as defined by risk assessment outcomes. USG organizations shall create and maintain documented operational processes managing the DNS infrastructure.

DNS Internal Security Requirements

1. USG organizations must have at a minimum one internal DNS system.
2. DNS systems must be physically and logically secured.
3. Internal hosts must resolve to an internal DNS server.
4. All servers and network equipment should have a static IP address that is assigned in DNS.
5. All internal applications should resolve to the internal DNS server.

DNS External Security Requirements

1. External DNS must be in a demilitarized zone (DMZ) or similar architecture.
2. External DNS must be protected with firewall equipment or intrusion prevention system (IPS).

3. Internet or external queries on the domain must be forwarded to an external DNS.
4. DNS systems must be physically and logically secured.

Section 5.14 Information Protection Management

Data are managed consistent with the organization's risk strategy to reduce cybersecurity risks, protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization). The loss of data privacy can, for example, result in identity theft. Identity theft is defined as a fraud committed or attempted using the identifying information of another person without authority. The risk to USG organizations and their faculty, staff, students, and other applicable constituents from identity theft and accompanying data loss is of significant concern to the USG. USG organizations should make reasonable efforts to detect, prevent, and mitigate identity theft.

5.14.1 Purpose

The USG adopts and implements this standard to detect, prevent, and mitigate identity theft, and to help protect USG organizations and their faculty, staff, students, and other applicable constituents from damages related to the loss or misuse of identifying information due to identity theft. Personal identifying information is defined in Section 5.7.⁷

Under this standard, USG organizations shall:

1. Identify patterns, practices, or specific activities (red flags) that could indicate the existence of identity theft with regard to new or existing covered accounts. A covered account is defined as:
 - Any account maintained by a USG organization for which there is a reasonably foreseeable risk of identity theft; or
 - Any reasonably foreseeable risk to the safety or soundness of the USG organization from identity theft, including financial, operational, compliance, reputation, or litigation risks; or
 - Any account that involves or is designated to permit multiple payments or transactions.
2. Respond appropriately to any red flags that are detected under this standard to prevent and mitigate identity theft.
3. Improve the protection process and ensure periodic updating of the standard, including reviewing the covered accounts and the identified red flags that are part of this standard.
4. Promote compliance with state and federal laws and regulations regarding information protection/identity theft protection.⁸

5.14.2 Identifying Red Flags

The following examples of red flags are potential indicators of fraud or identity theft. The risk factors for identifying relevant red flags include the types of covered accounts offered or maintained, the methods provided to open or access covered accounts, and previous experience with identity theft. Any time a red flag or a situation closely resembling a red flag is apparent, it should be investigated for verification.

⁷ O.C.G.A § 10-1-190 Identity Theft

⁸ Ibid

Suspicious Activity Concerning Identify Fraud

Examples of identity theft alerts, notifications, or warnings may include:

1. A report of fraud or active-duty alert in a credit or consumer report.
2. A notice of credit freeze from a credit or consumer reporting agency in response to a request for a credit or consumer report.
3. A notice of address discrepancy in response to a credit or consumer report request.
4. A credit or consumer report having a pattern of activity inconsistent with the history and usual pattern of activity of an applicant, such as:
 - A recent and significant increase in the volume of inquiries.
 - An unusual number of recently established credit relationships.
 - A material-change in the use of credit, especially in recently established credit relationships.
 - An account that was closed for cause or identified for abuse of account privileges.

Suspicious Documents

Examples of these red flags include:

1. Documents provided for identification appear to have been altered, forged, or are inauthentic.
2. The photograph or physical description on the identification document is inconsistent with the appearance of the individual presenting the identification.
3. Other information on the identification is inconsistent with information provided by the person opening a new covered account or individual presenting the identification.
4. Other information on the identification is inconsistent with readily accessible information that is on file with the USG organization, such as a signature card or a recent check.
5. An application appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

Examples of these red flags include:

1. Personal identifying information provided is inconsistent when compared against other sources of information used by the organization, such as:
 - The address does not match any address in the consumer report; or
 - The SSN has not been issued or is listed as deceased by the Social Security Administration.
2. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by that individual, such as a lack of correlation between the SSN range and date of birth.
3. Personal identifying information provided is associated with known fraudulent activity, such as the address or telephone number on an application is the same as one provided on a fraudulent application.
4. Personal identifying information provided is of a type commonly associated with fraudulent activity, such as:
 - The address on an application is fictitious, a mail drop, or a prison; or,

- The phone number is invalid or is associated with a pager or answering service.
- 5. The Social Security number provided is the same as one submitted by another person opening an account.
- 6. The address or telephone number provided is the same as or similar to the address or telephone number submitted by another person.
- 7. The individual opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- 8. Personal identifying information provided is inconsistent with personal identifying information that is on file with the USG organization.
- 9. When answering security questions (mother's maiden name, pet's name, etc.), the person opening that covered account cannot provide authenticating information beyond what would generally be available from a wallet or consumer report.

Suspicious Activity Related to a Covered Account with Financial Access

Examples of these red flags include:

1. Shortly following the notice of a change of address for a covered account, a request is received for a new, additional, or replacement card, or for the addition of authorized users on the account.
2. A covered account is used in a manner that is inconsistent with established patterns of activity on the account, such as nonpayment when there is no history of late or missed payments or a material-change in purchasing or usage patterns.
3. A covered account that has been inactive for a reasonably lengthy period of time is used, taking into consideration the type of account, the expected pattern of usage, and other relevant factors.
4. Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individual's covered account.
5. The USG organization is notified that the individual is not receiving paper account statements.
6. The USG organization is notified of unauthorized charges or transactions in connection with an individual's covered account.
7. The USG organization receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with its covered accounts.
8. The USG organization is notified by an employee or student, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
9. There is a breach in the USG organization's computer security system.

5.14.3 Detecting Red Flags

Student Enrollment

To detect red flags associated with the enrollment of a student, the USG organization will take the following steps to obtain and verify the identity of the individual opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address, or other identification; and,
2. Verify the student's identity at the time of issuance of the student identification card through review of a driver's license or other government-issued photo identification.

Existing Accounts

To detect red flags associated with an existing account, the USG organization will take the following steps to monitor transactions on an account:

1. Verify the identity of students if they request information;
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and,
3. Verify changes in banking information given for billing and payment purposes.

Background/Credit Report Requests

To detect red flags for an employment or volunteer position for which a credit or background report is sought, the USG organization will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and,
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made, and report to the consumer reporting agency an address for the applicant that has reasonably been confirmed is accurate.

5.14.4 Responding to Red Flags

Once detected, the USG organization must act quickly with consideration of the risk posed by the red flag. The USG organization should gather all related documentation quickly, write a description of the situation and present this information to the organizationally defined authority for determination. The organizationally defined authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic. The USG organization must activate their cybersecurity incident response plans as defined in Section 5.3.

5.14.5 Protecting Personal Information

To mitigate theft of personal information, USG organizations may take the following steps with respect to its internal operating procedures:

1. Lock file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with covered account information when not in use.
2. Lock storage rooms containing documents with covered account information and record retention areas at the end of each workday or when unsupervised.
3. Clear desks, workstations, work areas, printers, fax machines, and common shared work areas of all documents containing covered account information when not in use.
4. Destroy documents or computer files containing covered account or protected information in a secure manner. Note: Records may only be destroyed in accordance with the state's records retention guideline. Drawing on NIST 800-53 Media Sanitation controls:

- a. Media must be sanitized prior to disposal, released from organizational control, or released for reuse using organizationally defined sanitation techniques and procedures; and
 - b. Employ sanitation techniques and procedures with the strength and integrity commensurate with the security category or classification of the information stored.
5. Ensure that office computers with access to covered account information are password protected.
6. Ensure that the endpoint is secure.
7. Avoid the use of social security numbers (SSN) except when deemed essential for business functions.
8. Use encryption devices or protocols when transmitting covered account or protected information.
9. Evaluate the effectiveness of the steps above and implement the principle of continuous improvement.

This section should be read in conjunction with the Family Education Rights and Privacy Act (FERPA), the Georgia Open Records Act, and other applicable laws and policies. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor or USG Cybersecurity for advice.

Section 5.15 Email Use and Protection

5.15.1 Purpose

USG organizations provide email services to USG faculty and staff to assist those employees in facilitating state business and communicating on matters of official business. USG organizations also provide email services to students upon actual or planned enrollment and for a period after the student completes his or her studies. This section establishes a standard for the appropriate use and protection of USG email systems.

5.15.2 Requirements

1. USG employee email accounts should be used primarily for organizational business-related purposes; personal communication is permitted on a limited basis for use incidental to the employee's job duties and responsibilities.
2. USG employees may not use USG and institution employee email accounts for commercial solicitation or in furtherance of partisan political activity.
3. Access to email shall be governed by the USG organization's authorization and access control and password protection policies and standards.
4. Email passwords shall be encrypted and not be stored or transmitted in clear text.
5. Email systems shall be protected from viruses, interception, and other malicious intentions.
6. Email forwarding must be verified by the email account user or the USG organization's executive management.

7. All USG organizations shall implement email platforms using an approved cloud solutions provider. Exceptions should be documented as stated in the *Introduction, Exceptions* of this document.
8. Reference *Human Resources Administrative Practice Manual*⁹ for actions taken when employees are terminated or separated. For account management, reference the USG *IT Handbook* Section 3.1.

5.15.3 Retiree Email Account Management

USG organizations may have chosen to permit users to retain their email addresses upon departure or retirement. As threat landscapes change, USG organizations shall review these practices as concerns emerge pertaining to organization reputation and representation – as defined in *BOR Policy 8.2.8.3*.¹⁰ Examples are:

Business Impact:

- Loss of potentially important if not protected business information when an employee (associated with the role) departs or retires.
- Potential organizational liability associated with these accounts when misused. The user may no longer be subject to following USG policy.

Cyber Threat:

- Spoof/masquerade attacks pretended to be the owner of the account to defraud or mislead. This is the basis for business email compromise (BEC) attacks.
- Phishing is the number one way an attacker steals credentials.

If retirees are permitted to access USG email resources, USG organizations must create and publicize appropriate policies and guidelines delineating responsibilities to ensure appropriate security.

Responsibilities for any USG organization permitting retiree email should include, at a minimum:

- Determining the business need where email is permitted.
- Conducting a risk assessment concerning the permitted email.
- Detailing the types of data protection and security required.
- Defining the minimum level of access controls (least privilege).
- Communicating a clear distinction to the public regarding the role of the individual. Examples include:
 - Retirees may be identified in their email signature, e.g., Dr. Sally Smith, Professor Emeritus or Dr. James Jay, retired; or
 - USG organizations may consider unique email domains (e.g., username@retired.usg.edu).
- Providing a disclaimer of liability for personal data loss.
- Notifying users of disclosure requirements under the Georgia Open Records Act; and

⁹ <https://www.usg.edu/hr/manual/>

¹⁰ <https://www.usg.edu/policymanual/>

- Disabling and deleting retiree email accounts after a specified period of inactivity and other organizationally defined triggers.

Retiree email accounts should be used primarily for organizational business-related purposes; personal communication is permitted on a limited basis for use incidental to the employee's job duties and responsibilities. Retirees must agree not to use this resource for any criminal purposes, partisan political activity, or other use inconsistent with federal and state law, etc.

USG organizations reserve the right to terminate access to email service if the user violates BOR Policy.

Section 6 Data Privacy

Section Control

Table 6.1: Revision History

Date	Description of Change
05/02/2016	Initial redesign referenced in a new structure and format. PDF, structure and format.
07/09/2020	Align with NIST Privacy Framework and NIST CSF Framework. Rename Section 6 to "Data Privacy".
07/09/2020	Provide IT Handbook portion of USG data privacy program. Add Section 6.3 Data Privacy Risks.

Table 6.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date	Revision Date(s)
6.1	USG Data Privacy Standard	June 2013	May 2014	May 2014	July 2020
6.2	USG Web Privacy Standard	June 2013	May 2014	May 2014	July 2020
6.3	Data Privacy Risks	July 2020	August 2020	TBD	N/A

Introduction

This section outlines data privacy requirements for USG organizations. The USG is committed to protecting privacy. Personal information will only be disclosed to third parties when allowed by law or with the consent of the data subject.

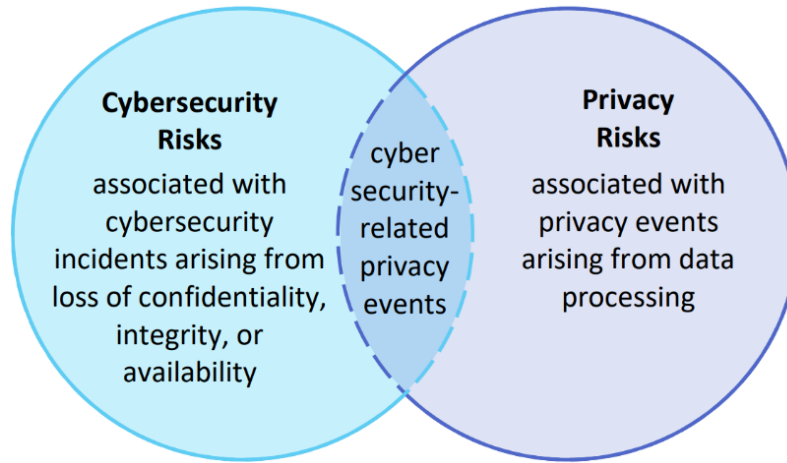


Figure 5: Risk Relationship Diagram – Cybersecurity and Privacy ¹¹

Since its adoption, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) has helped USG organizations to communicate and manage cybersecurity risk. While managing cybersecurity risk contributes to managing privacy risk, it is not enough, as privacy risks can also arise by means unrelated to cybersecurity incidents, as illustrated by **Figure 5**. Having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. The scope of this section concerns “Privacy Risks” functions that are technology-related systems, products, or services.

Section 6.1 USG Data Privacy Standard

6.1.1 Purpose

This section defines general data privacy requirements for all USG organizations.

6.1.2 Standard

All USG organizations shall enact and maintain permanent data privacy processes and procedures in adherence with this standard, which includes, but is not limited to, the following principles:

1. Personally identifiable information (PII) may only be obtained through lawful means or with the consent of the data subject.
2. The purposes for which personally identifiable data are collected must be specified at or prior to the time of collection, and any subsequent use of the data shall be limited to and consistent with the fulfillment of those purposes previously specified.
3. Personal data may not be disclosed, made available, or otherwise used for a purpose other than those specified, except with the consent of the subject of the data, or as allowed by statute or regulation.
4. Personal data collected must be relevant to the purpose for which it is needed.

¹¹ NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0, January 116, 2020

5. The general means by which personal data is protected against loss, unauthorized access, use, modification or disclosure must be posted, unless the disclosure of those general means would compromise legitimate USG entity objectives or law enforcement purposes.

6.1.3 Applicability and Compliance

Each USG organization must implement the data privacy standard by:

1. Designating a position responsible for the implementation of and adherence to the standard.
2. Posting the standard prominently in offices and on the intranet website, if site exists.
3. Distributing the standard to each employee and contractor who has access to personal data.
4. Complying with the USG Data Privacy Standard and all other State and Federal laws pertaining to data privacy.
5. Using appropriate means to successfully implement and adhere to the standard.

Section 6.2 USG Web Privacy Standard

By accessing any website of any USG organization, users agree to abide by this web privacy standard, as well as the USG *IT Handbook*.

6.2.1 Information Collection and Use

The USG may collect some information (analytic data) about how visitors' access and use a website affiliated with the USG.EDU domain and its contents. The information collected on any such website is limited to non-personally identifiable information and may include information such as the computer IP/MAC addresses and browser information used to access the website. These data are used to improve website content and website management for users. Cookies may be used to facilitate the navigation of this site, but these cookies will not contain any personally identifiable information. Other USG websites may have different privacy practices. If applicable, consult the privacy statement on each website.

Section 6.3 Data Privacy Risks

The Privacy Framework approach to privacy risk is to consider privacy events as potential problems USG organizations could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal.

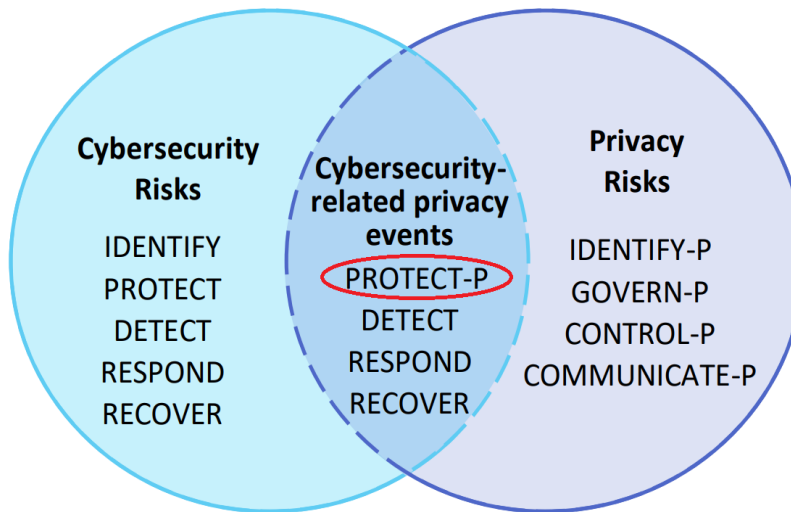


Figure 6: Using NIST Frameworks to Manage Cybersecurity and Privacy Risks ¹²

The *USG IT Handbook* was adapted to align with the CSF. The CSF, although intended to cover all types of cybersecurity incidents, can be leveraged to further support the management of risks associated with cybersecurity-related privacy events. The Protect-P function, circled in red (**Figure 6**), is specifically focused on managing risks associated with cybersecurity-related privacy events (e.g., *privacy breaches*) and is integrated into the *USG IT Handbook*. USG organizations shall use all five of the CSF functions in conjunction with Identify-P, Govern-P, and Control-P, to collectively address technical data privacy and cybersecurity risks. The “Privacy Risk” functions that are business-related are referenced in the *USG Business Procedures Manual (BPM)*, *Sec 12: Data Privacy*. The Communicate-P function is entirely located within the BPM. For additional guidance, reference the *USG IT Handbook Crosswalk* and the *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*.

6.3.1 IDENTIFY-P

To address “Inventory and Mapping” requirements, USG organizations shall develop the organizational understanding to manage privacy risk for individuals arising from data processing by ensuring data processing by systems, products or services is understood and informs the leadership of privacy risk. To demonstrate this understanding, USG organizations shall ensure:

1. Owners or operators (e.g., the organization and/or third parties such as service providers, partners, customers and developers) and their roles with respect to the systems, products, services and components (e.g., internal or external) that process data are inventoried;
2. The data processing environment is identified (e.g., geographic location, internal, cloud or third parties); and,
3. Data processing is mapped, illustrating the data actions and associated data elements for systems, products and services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems, products and services.

To address the “Business Environment” requirements, USG organizations must ensure mission, objectives, stakeholders and activities are understood and prioritized; this information is used to inform

¹² NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0, January 116, 2020

privacy roles, responsibilities and risk management decisions, which includes verifying systems, products and services that support organizational priorities are identified and key requirements communicated.

6.3.2 GOVERN-P

USG organizations shall develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk. To address the "Governance Policies, Processes, and Procedures" requirements, the documentation to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management of privacy risk. USG organizations can accomplish this by ensuring the roles and responsibilities for the workforce are established with respect to data privacy.

6.3.3 CONTROL-P

USG Organizations shall develop and implement appropriate activities to enable organizations or individuals to manage data with enough granularity to manage privacy risks. To address the "Data Processing Management" requirements, data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization). This is accomplished by ensuring the technical measures implemented to manage data processing are tested and assessed.

Section 7 Facilities

Section Control

Table 7.1: Revision History

Date	Name	Description of Change
05/02/2016	PDF, structure, and format	Initial redesign referenced in a new structure and format.
05/11/2021	Physical and Environmental Security	Added subsection to cover physical security in advance of contingency planning.

Table 7.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date
7.1	Physical and Environmental Security	05/11/2021	TBD	TBD

Introduction

Protection for on-premises information systems and personnel requires appropriately designed and managed facilities where information systems reside. Information systems include resources organized for the collection, processing, maintenance, use, sharing, dissemination, and disposition of information, which also includes telephony and environmental control systems. Managing a physical environment includes defining the site requirements, selecting the appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces injury to personnel and business interruptions from damage to information systems.

7.1 Physical and Environmental Security

The following has been modeled on *NIST SP800-53 (Rev4) Physical and Environmental Protection (PE)* Family. USG organizations must perform a risk assessment to determine the applicability of the following safeguards.

Requirements

If applicable, USG organizations shall implement physical and environmental protection procedures that include the following safeguards:

1. Develop documentation that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, then:
 - a. Disseminate to organization-defined personnel or roles; and,
 - b. Review and update according to an organization-defined frequency.
2. Review, approve, and maintain an inventory of individuals with authorized access to the facilities where the information systems reside by:
 - a. Issuing authorization credentials for facilities access;
 - b. Reviewing the access list detailing authorized facilities access by individuals on an organization-defined frequency; and,

- c. Removing individuals from the facilities access list when access is no longer required.
- 3. Enforce physical access authorizations at organization-defined entry/exit points to the facilities where information systems reside by:
 - a. Verifying individual access authorizations before granting access to the facilities;
 - b. Controlling ingress/egress to the facilities;
 - c. Maintaining physical access audit logs following an organization-defined period;
 - d. Escorting visitors and monitoring visitor activity;
 - e. Securing keys, combinations, and other physical access devices;
 - f. Inventorying physical access devices on an organization-defined frequency; and,
 - g. Changing combinations and keys following an organization-defined frequency and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
- 4. Monitor physical access to the facilities where information systems reside to detect and respond to physical security incidents by reviewing physical access logs upon frequency or occurrence of an organization-defined event.
- 5. Ensure an emergency power off (EPO) control is available to protect the facilities' personnel and system components; and ensure the EPO is protected from unauthorized activation and test following an organization-defined frequency.
- 6. Ensure a short-term or long-term uninterruptible power source is available to either facilitate an orderly shutdown or transition to an alternate power source and test following an organization-defined frequency.
- 7. Ensure an automatic emergency lighting solution has been implemented that activates in the event of a power outage or disruption that covers emergency exits and evacuation routes and test following an organization-defined frequency.
- 8. Implement fire suppression and detection solutions for information systems that are activated by an independent energy source and inspected by a licensed and approved party.
- 9. Ensure environmental temperature and humidity controls are monitored and maintained in accordance with equipment specifications.
- 10. Ensure information systems are protected from water damage by installing shutoff and/or bypass valves and drainage systems that are accessible to authorized personnel, clearly labeled, and test following an organization-defined frequency.
- 11. Authorize, inventory, monitor, and control organization-defined types of information system components entering and exiting the facilities and maintain records of those items.
- 12. Plan, implement, manage, and monitor the above applicable safeguards at the organization-defined alternate work sites; and assess as feasible, the effectiveness of the safeguards at alternate work sites.

Section 8 Bring Your Own Device (BYOD) Standard

Section Control

Table 8.1: Revision History

Date	Description of Change
05/02/2016	Initial redesign referenced in a new structure and format. PDF, structure and format.

Table 8.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date	Revision Date(s)
8.1	Purpose	October 2013	October 2013	October 2014	
8.2	Applicability	October 2013	October 2013	October 2014	January 2014
8.3	Standards	October 2013	October 2013	October 2014	
8.4	Standard Non-Compliance	October 2013	October 2013	October 2014	
8.5	Appendix A: Employee Declaration	October 2013	October 2013	October 2014	

Introduction

This section establishes the standards and procedures for end users who are connecting a personally owned device to a USG network for business purposes.

Section 8.1 Purpose

The purpose of this standard is to empower USG staff to innovate and work on USG business more effectively inside and outside the office. Based on research at other enterprises, greater productivity and employee satisfaction should result from establishing a prudent BYOD standard that empowers employees to work on personally owned devices while protecting the confidentiality, integrity and availability of USG data. This standard intends to balance the use of personally owned devices while preventing USG data from being deliberately or inadvertently stored insecurely on a device or carried over an insecure network where it could potentially be accessed by unauthorized resources. Such a breach could result in loss of information, damage to critical applications, financial loss and damage to the USG's public image. Therefore, all users employing a personally owned device connected to a USG network, and/or capable of backing up, storing, or otherwise accessing USG data of any type, must adhere to USG-defined policies, standards and processes.

Section 8.2 Applicability

This standard applies to all USG employees, including full- and part-time staff, consultants and other agents who use a personally owned device to access, store, backup or relocate any USG or client-specific data. Such access to these data is a privilege, not a right, and forms the basis of a trust the USG has built with its clients, vendor partners and other constituents. Consequently, USG employment does not automatically guarantee the initial or ongoing ability to use these devices to gain access to USG

networks and information. This standard applies to any hardware and related software that is not owned or supplied by the USG but could be used to access USG resources. This includes devices that employees have acquired for personal use, but also wish to use in the business environment. It includes any personally owned device capable of inputting, processing, storing and outputting USG data. This standard is complementary to any previously implemented policies and standards covering acceptable use, data access, data storage, data movement and processing, and connectivity of devices to any element of the enterprise network. Always consult the USG Information Technology Handbook for up-to-date standards and guidance.

Section 8.3 Standards

8.3.1 Prior Approval

1. Employees using personally owned devices, software, and/or related components to access USG data will ensure such devices employ some sort of device access protection such as, but not limited to, passcode, facial recognition, card swipe, etc. Within the USO, this approval authority is delegated to the first vice chancellor or above in the employee's chain of command in consultation with the USG CIO. USG organizations will establish and document local policies consistent with this prior approval standard.
2. USG organizations will establish consistent, documented, and repeatable processes that are consistent with this prior approval standard and can be considered auditable.

8.3.2 Security

1. Employees using prior-approved personally owned devices and related software shall make every attempt to keep these devices and related software protected.
2. Employees using prior-approved personally owned devices and related software accessing sensitive data will, in addition to device access protection, ensure that the sensitive data is protected using data encryption or USG-provided mobile device management, or the equivalent.
3. Determination of equivalent measures is reserved to the USG CISO, ISOs of the USG organizations, and/or other delegated designees. USG organizations will need to document evidence of compliance.
4. Passwords and/or other sensitive data will not be stored unencrypted on mobile devices.
5. Managers will implement a documented process by which employees acknowledge and confirm to have all USG-sensitive data permanently erased from their personally owned devices once their use is no longer required, as defined in Section 8.2.
6. Employees agree to and accept that their access to USG networks may be monitored to identify unusual usage patterns or other suspicious activity. This monitoring is necessary to identify accounts/computers that may have been compromised by external parties.
7. Employees will immediately report to their managers any incident or suspected incidents of unauthorized data access, data or device loss and/or disclosure of system or USG organization resources as it relates to personally owned devices.
8. Managers will immediately report such incidents to the USG CISO or the organization's ISO as appropriate.

8.3.3 USG Intellectual Property

1. The principal storage location of state-owned data is a state-owned or contracted resource.
2. Sensitive state-owned data may not be stored on external cloud-based personal accounts.

8.3.4 Device and Application Support

1. Personally owned devices and software are not eligible for support from USG departments.
2. Employees will make no modifications to personally owned hardware or software that circumvents established USG security protocols in a significant way (e.g., replacing or overriding the operating system or “jail-breaking”).

Section 8.4 Standard Non-Compliance

Failure to comply with the USG BYOD standard may, at the full discretion of the USG organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.

Section 8.5 Employee Declaration Template

I, _____, have read and understand the USG BYOD standard and any augmenting USG organization standards, and consent to adhere to the standards and procedures outlined therein. I, [_____] approve of the use of personal devices by this employee.

Employee Signature	Date
--------------------	------

Supervisor Signature	Date
----------------------	------

Approval Authority Signature	Date
------------------------------	------

Section 9 Open for Future Use

Data Governance and Management was relocated to Section 12 of the Business Procedures Manual.

Section 10 Learning Management System (LMS)

Section Control

Table 10.1: Revision History

Date	Name	Description of Change
05/02/2016	PDF, structure, and format	Initial redesign referenced in a new structure and format.
03/15/2021	Content revisions	Revised Service Description, Participation Model, Business Owner, General Description, Annual Escalator, and Change Management sections. Removed LMS Executive Committee and added Institutional Oversight. Removed Equipment Refresh due to LMS cloud hosting.

Table 10.2: Compliance

Section Number	Section Name	Compilation Date	Published Date	Compliance Date
10.1	Service Description	March 2021	September 2021	September 2021
10.2	Governance and Institutional Oversight	March 2021	September 2021	September 2021
10.3	Resources Model	March 2021	September 2021	September 2021
10.4	Change Management	March 2021	September 2021	September 2021
10.5	Third Party Integration	March 2021	September 2021	September 2021

Introduction

This section introduces the USG Learning Management System (LMS), a managed service being provided by USG Information Technology Services on behalf of the USG. The LMS service leverages economies of scale and enhances operational efficiencies considerably while increasing access and stability of LMS applications across all institutions. This standard applies to USG organizations.

10.1 Service Description

Services provided and managed as part of the GeorgiaVIEW LMS align with the USG *Service Level Guidelines*. The system standard for the LMS is D2L Brightspace. USG institutions or units desiring to use state resources to support a different system require the written approval of the Chancellor. Such requests will be routed through the USG CIO, vice chancellor for academic affairs, and the executive vice chancellor and chief academic officer to the chancellor. All institutions should have one LMS for all of their faculty and students, regardless of academic discipline. The students of the USG were very clear that they strongly prefer a unified LMS platform on their respective campus.

10.2 Governance and Institutional Oversight

USG Academic Affairs is the business owner of the LMS. Additionally, D2L Brightspace utilizes configuration variables for many settings, which allow institutional administrators to adjust LMS functionality for their environment. Additionally, highly impactful changes (as deemed by D2L) come

with a default of “off,” so institutions may have time to assess when is most appropriate to activate such features. Through the GeorgiaVIEW Functional Advisory Committee (GFAC), USG institutions can recommend the best timing of highly impactful changes to the LMS.

10.3 Resource Model

The LMS service leverages economies of scale and enhances operational efficiencies considerably while increasing access and stability of LMS applications across all institutions. The key financial principles of the system wide LMS deployment are: 1) The LMS is funded through revenue chargeback to the institutions, and 2) To preserve the economies of scale, all institutions are required to participate in this effort and should use D2L exclusively as their LMS. However, if an institution wishes to offer an independent and local LMS program, they must formally petition the chancellor. If approved, the institution remains responsible for their portion and payment of the USG LMS program costs. Otherwise, other USG institutions would be penalized as institutions entered or departed the program.

10.3.1 Licensing and Hosting Costs

The revenue chargeback is based on the institutional FTE. The base license and hosting costs, for all institutions except the Georgia Institute of Technology, are included in funds allocated to institutions. These funds include resources provided to cover the previous LMS costs and additional funds provided to cover the differential cost of the current system. The total of these two different funding sources covers the LMS licensing and hosting costs. The Georgia Institute of Technology was granted a waiver to continue on its current LMS and, thus, is responsible for its own hosting and licensing costs. All waivers will be reviewed periodically by USG Academic Affairs to consider the utility of continuing the waiver.

10.4 Change Management

Upgrades to the LMS occur monthly, typically with no downtime, aligning with D2L’s continuous delivery model. Continuous delivery is a design practice used in software development to automate and improve the process of software delivery. The continuous delivery model allows D2L to deliver updated technology to clients, enabling rapid, incremental delivery of high quality, valuable new functionality to users. This frictionless model also makes it possible to increase collaboration with clients and to adapt software in line with user feedback and needs, resulting in incremental and easily integrated changes. D2L will be encouraged to work with USG institutions so that highly impactful changes occur in months in which they will have the least disruption to educational operations. These may include, but not be limited to, May, July, and December, months of semester transitions. By acting as a consortium, institutions can realize additional savings by purchasing additional functionality in the LMS.

10.5 Supplier Integration

Supplier or third-party vendor integrations into the LMS will be at the discretion of the institution. However, to further leverage economies of scale and enhance operational efficiencies, USG ITS may enter into service level agreements which may restrict the choice of supplier’s institutions have for third party integrations. All integrations into the LMS will require the supplier to complete the latest version of the USG Third Party Vendor Questionnaire. This questionnaire will be reviewed by GeorgiaVIEW and USG Cybersecurity staff who will issue recommendations back to the institution regarding activation of the integration in the LMS production environment.

Appendix A: References

- Board of Regents, University System of Georgia - Policies <https://www.usg.edu/policies>
 - Policy Manual - Section 10
 - Business Procedures Manual
 - Data Privacy Policy and Legal Notice
 - Ethics & Compliance Program
 - Records Management and Archives - Records Retention Schedule
- Federal Regulation & Legislation <https://www.govinfo.gov/> | <https://www.cnss.gov/> | <https://www.whitehouse.gov/omb/> | <https://www.irs.gov/>
 - Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014.
 - Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015.
 - Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017.
 - Federal Information Policy, 44 U.S.C, Sec 3502 (8)
 - Federal Information Security Modernization Act (P.L. 113-283), December 2014.
 - Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended by Public Law No. 104-231, 110 Stat. 3048
 - Electronic Freedom of Information Act Amendments of 1996.
 - Internal Revenue Service, IRS Publication 1075.
 - Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
 - Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 2016.
 - Office of Management and Budget Memorandum M-13-13, *Open Data Policy-Managing Information as an Asset*, May 2013.
 - Office of Management and Budget Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017.
 - Office of Management and Budget Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, December 2018.
 - Privacy Act (P.L. 93-579), December 1974.
 - Title 21 Code of Federal Regulations, 21.
 - Title 32 Code of Federal Regulations, Sec. 2002.4, Definitions. 2018 Ed.
 - Title 40 U.S. Code, Sec. 11331, *Responsibilities for Federal information systems standards*. 2017 Ed.

- Title 44 U.S. Code, Sec. 3301, Definition of records. 2017 Ed.
- Title 44 U.S. Code, Sec. 3502, Definitions. 2017 Ed.
- Title 44 U.S. Code, Sec. 3552, Definitions. 2017 Ed.
- Title 44 U.S. Code, Sec. 3554, Federal agency responsibilities. 2017 Ed.
- Title 44 U.S. Code, Sec. 3601, Definitions. 2017 Ed.
- Industry Standards and Best Practices <https://iso.org/> | <https://technet.microsoft.com/> | <https://www.archives.gov/cui> | <https://www.aicpa.org/>
 - ISO 27005 Information Security Risk Management (ISRM)
 - Microsoft Securing DNS
 - National Archives and Records Administration, Controlled Unclassified Information (CUI) Registry.
 - Generally Accepted Privacy Principles (GAPP)
- NIST Computer Security Resource Center - FIPS <https://csrc.nist.gov/publications/fips>
 - FIPS Publication 199, *Standards for Security Categorization for Federal Information Systems*, February 2004.
 - FIPS Publication 200, *Minimum Security Requirements for Federal Information Systems*, March 2016.
- NIST Computer Security Resource Center - Glossary <https://csrc.nist.gov/glossary>
- NIST Computer Security Resource Center - SP <https://csrc.nist.gov/publications/sp>
 - SP 800-16 *IT Security Training Requirements*, April 1998.
 - SP 800-18 Rev. 1 *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
 - SP 800-28 Ver. 2 *Guidelines on Active Content and Mobile Code*, March 2008.
 - SP 800-30 Rev. 1 *Guide for Conducting Risk Assessments*, September 2012.
 - SP 800-34 Rev. 1 *Contingency Planning Guide for Federal Information Systems*
 - SP 800-37 Rev. 1 *Guide for Applying the Risk Management Framework...*
 - SP 800-50 *Building an IT Security Awareness and Training Program*, October 2003.
 - SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
 - SP 800-53A *Assessing Security and Privacy Controls: Building Effective Security Assessment Plans*, July 2008.
 - SP 800-55 *Performance Measurement Guide for Information Security*, December 2014.
 - SP 800-60 Vol 1&2 Rev. 1 *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
 - SP 800-61 Rev. 2 *Computer Security Incident Handling Guide*, August 2012.

- SP 800-81-2 *Secure Domain Name System (DNS) Deployment Guide*, September 2013.
- SP 800-83 Rev. 1 *Guide to Malware Incident Prevention and Handling*, July 2013.
- SP 800-92 *Guide to Computer Security Log Management*, September 2006.
- SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.
- SP 800-181 Rev. 1 *National Initiative for Cybersecurity Education (NICE)*.
- NIST Frameworks
 - Cybersecurity Framework <https://www.nist.gov/cyberframework>
 - Privacy Framework <https://www.nist.gov/privacy-framework>
- NIST Interagency/Internal Report - IR <https://csrc.nist.gov/publications/nistir>
 - NISTIR 8259 *Baseline for Securable IoT Devices*, May 2020.
- Official Code of Georgia Annotated <http://www.lexisnexis.com/hottopics/gacode/default.asp>
 - O.C.G.A. § 10-1-910 – *Identity Theft*
 - O.C.G.A § 16-9-90, et seq. – *Georgia Computer Systems Protection Act*
 - O.C.G.A. § 16-9-150 – *Georgia Computer Security Act of 2005*
 - O.C.G.A § 50-18-72 – *Georgia Open Records Act*
 - O.C.G.A. § 38-3-22 (2021 Cyber incident reporting responsibilities.)

Appendix B: Glossary

Abuse	Activity that violates an organization's Acceptable Use Policy (AUP).
Access Control	The process of permitting or restricting access to applications at a granular level, such as per-user, per-group, and per-resources. (Source: SP 800-113)
Architecture	A set of related physical and logical representations (i.e., views) of a system or a solution. The architecture conveys information about system/solution elements, interconnections, relationships, and behavior at different levels of abstractions and with different scopes. Refer to security architecture. (Source: SP 800-160)
Assurance	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (Source: SP 800-39)
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality. (Source: SP 800-82 Rev. 2)
Authentication	A process of attempting to verify the digital identity of a system user or processes. (Source: SP 800-47)
Availability	Ensures timely and reliable access to and use of information. (Source: SP 800-137; 44 U.S.C., Sec. 3542)
Awareness	Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance. (Source: SP 800-50)
Awareness, Training, and Education Controls	Include (1) awareness programs which set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure, (2) training which teaches people the skills that will enable them to perform their jobs more effectively, and (3) education which is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities. (Source: SP 800-16)

Baseline	Formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle. Note: The engineering process generates many artifacts that are maintained as a baseline over the course of the engineering effort and after its completion. The configuration control processes of the engineering effort manage baselined artifacts. Examples include stakeholder requirements baseline, system requirements baseline, architecture/design baseline, and configuration baseline. (Source: SP 800-160)
Benign Policy Violation	Activity that violates organizational Acceptable Use Policy (AUP) but is not a threat and requires no action.
Bring Your Own Device (BYOD)	Refers to employees taking their own personal device to work to interface to the USG organization's network resources.
Brute Force Attack	In cryptography, an attack that involves trying all possible combinations to find a match. A method of accessing an obstructed device through attempting multiple combinations of numeric/alphanumeric passwords. (Source: SP 800-72)
Business Case	A description of a requested project or initiative that explains the goals, benefits, and cost of the request.
Business Continuity Plan	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. (Source: SP 800-34 Rev.1)
Business Impact Analysis	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (Source: SP 800-34 Rev. 1)
Certificate	A data structure that contains an entity's identifier(s), the entity's public key (including an indication of the associated set of domain parameters) and possibly other information, along with a signature on that data set that is generated by a trusted party, i.e. a certificate authority, thereby binding the public key to the included identifier(s). (Source: SP 800-56A Rev. 2)
Certificate Authority	A trusted entity that issues and revokes public key certificates. (Source: SP 800-63-2)
Chain of Custody	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. (Source: 800-72)

Chief Information Officer (CIO)	Organization official responsible for: 1) providing advice and other assistance to organization senior leadership to ensure that information systems are acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the organization presidents, chancellor, or the Board of Regents; 2) developing, maintaining, and facilitating the implementation of a sound and integrated information system architecture; and 3) promoting the effective and efficient design and operation of all major information resources management processes, including improvements to work processes. (Source: SP 800-53)
Chief Information Security Officer (CISO)	Organization official responsible for: 1) developing and maintaining a cybersecurity organization and architecture in support of cybersecurity across the USG and between USG institutions; and 2) maintaining cybersecurity implementation guidelines that the USO, all USG institutions, and the GPLS shall follow in the development of their individualized cybersecurity plans. (Source: BOR Policy Manual)
Classified Information	Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD). (Source: SP 800-53 Rev. 4)
Common Control	A security control that is inherited by one or more organizational information systems. See Security Control Inheritance. (Source: SP 800-137)
Compensating Controls	The cybersecurity or privacy controls or safeguards implemented in lieu of the baseline controls that provide equivalent or comparable protection for a system or organization.
Compliance Date	The date by which the USG organization is expected to comply with the policy or standard.
Compromise	The unauthorized disclosure, modification or use of sensitive data (e.g., keying material and other security-related information). (Source: SP 800-133)
Confidential Data	Data for which restrictions on the accessibility and dissemination of information are in effect. This includes information whose improper use or disclosure could adversely affect the ability of the institution to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of

	1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.
Confidentiality	Preserves authorized restrictions on information access and disclosure and includes means for protecting personal privacy and proprietary information. (Source SP 800-137)
Context of Use	The purpose for which PII is collected, stored, used, processed, described, or disseminated.
Continuity of Operations Plan	A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days because of a disaster event before returning to normal operations. (Source: SP 800-34 Rev. 1)
Controlled Unclassified Information (CUI)	A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. (Source: SP 800-53 Rev. 4)
Controls	<p>Controls, also known as safeguards, are proactive measures prescribed to meet the security requirements specified for an information system.</p> <ol style="list-style-type: none"> 1. Administrative Controls 2. Technical Controls 3. Physical Controls
Critical System	Reference "Mission-Critical System."
Critical System/Infrastructure	System and/or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source: SP 800-30 Rev. 1)
Cybersecurity	The role of cybersecurity is to understand, implement and manage safeguards that prevent, detect and deter risks to systems, products and services that store, transmit and process data.
Cybersecurity Incident	Cybersecurity Incident is a violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

Data Actions	A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal. (NIST IR 8062)
Data Element:	The smallest named item of data that conveys meaningful information. (NIST PF)
Data Leak/Leakage	An unauthorized transmission of data from within an organization to an external destination or recipient.
Data Privacy	The practices which ensure that the data shared by customers is only used for its intended purpose.
Data Processing	The collective set of data actions (NIST IR 8062)
Data Processing Ecosystem	The interconnected relationships among entities involved in creating or deploying systems, products or services or any components that process data. (NIST PF)
Data at Rest	Computer files that are used as reference, but are not often, if at all, updated. They may reside on servers, in backup storage or on the user's own hard disk.
Data Subject	Any person whose personal data is being collected, held or processed.
Data Subject Request	A DSR is a petition to an organization by a data subject looking to confirm whether or not the organization is holding personal data about the data subject petitioning, and if so, the data subject has the right to access that data, amend that data, or where permitted by law request for that his/her data be erased.
Data in Transit	Data on the move from origin or source to destination.
Data Integrity	A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored. In this Recommendation, the statement that a cryptographic algorithm "provides data integrity" means that the algorithm is used to detect unauthorized alterations. (Source: SP 800-56B Rev.1)
Data Leakage	The unauthorized or unintended transmission of data from within an organization to an external destination or recipient.
Data Loss	The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. (Source: SP 800-137)

Data Loss Prevention	A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of protected/classified/CUI information. (Source: CNSSI 4009-2015)
Data Spillage	An accidental or deliberate cybersecurity incident that results in the transfer of classified information onto an information system not authorized to store or process that information. (Source CNSSI 4009-2015)
Data Steward	Data Steward is defined in section 9.2 of the Information Technology Handbook. Examples are the registrar and director of human resources (HR).
De-identified Information	Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.
Denial of Service	Activity involving an attempt to make a resource unavailable to your network. (Source: SP 800-33)
Disassociated Processing	Or disassociability, enables the processing of data or events without association to individuals or devices beyond the operational requirements of the system (NIST IR 8062)
DNS Spoofing	DNS Spoofing refers to confusing a DNS server into giving out bad information.
Domain	Domain is most often used to refer to a domain zone; it is also used to describe a zone or a domain name.
Domain Name Service (DNS)	DNS refers to the domain name system, which represents a powerful Internet technology for converting domain names to their corresponding IP addresses.
Dwell Time	The time calculated as the number of days an adversary is present on a victim network, from first evidence of compromise to detection.
Endpoint Security	Endpoint Security is an approach to network protection that requires each computing device on a corporate network to comply with certain standards before network access is granted. Simple

forms of endpoint security include personal firewalls or anti-virus software that is distributed and then monitored and updated from a server. (Source: SP 800-128)

Endpoint Security Management

Endpoint Security Management is a policy-based approach to network security that requires endpoint devices to comply with specific criteria before they are granted access to network resources.

Endpoint Security Management Systems

Endpoint Security Management Systems, which can be purchased as software or as a dedicated appliance, discover, manage, and control computing devices that request access to the corporate network. Endpoints that do not comply with policy can be controlled by the system to varying degrees. For example, the system may remove local administrative rights or restrict Internet browsing capabilities.

Endpoints

Endpoints can include, but are not limited to, PCs, laptops, smart phones, tablets and specialized equipment such as bar code readers or point of sale (POS) terminals.

Enterprise

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See Organization. (Source: SP 800-30)

Event

A questionable or suspicious activity that could threaten the security objectives for critical or sensitive data or infrastructure. They may or may not have criminal implications. (Source: SP 800-160)

Exploit Attempt

Activity involving an attempt execute a specific flaw (vulnerability.)

False Positive

Activity that matches the specified criteria but is not an actual threat or vulnerability. (Source: SP 800-115)

General Support System (GSS)

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. (Source: SP 800-18 Rev. 1)

Guideline

A guideline is a document that suggests a path or guidance on how to achieve or reach compliance with a policy.

Harm	Any adverse effects that would be experienced by an individual or an organization if the confidentiality of PII were breached.
Host infection, Trojan, or Malware	Activity involving a possible host infection, Trojan infection, or malware intrusion.
Health Information	Any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. (Source: SP 800-66 Rev. 1)
Human Resource Management	Human Resource Management (HRM) is the area of administrative focus pertaining to an organization's employees. HRM is sometimes referred to simply as HR.
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (Source: SP 800-34 Rev. 1)
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (Source: SP 800-53 Rev. 4)
Incident Response Management	Process of detecting, mitigating, and analyzing threats or violations of cybersecurity policies and limiting their effect.
Information Leakage	Intentional or unintentional activity that could result in the transmission of data to unauthorized parties. (Source: SP 800-53 Rev. 4)
Information Security Officer (ISO)	Organization official responsible for: 1) maintaining the cybersecurity of different types of information within the organization that typically involves maintaining computer networks to ensure that sensitive financial or private information is kept secure and cannot be accessed by someone not authorized to do so; 2) that usually reports to a chief information security officer or other member of upper management, such as a vice president in charge of information technology (IT) or cybersecurity.

Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. (Source: SP 800-137)
Institutional Investigation	Activity reported by an institution in accordance with their incident response plans.
Isolated Event	Activity that is isolated or the context is undetermined.
Issues	A problem impacting the successful outcome of a project. Project issues should be tracked through resolution.
Linkable Information	Information about or related to an individual for which there is a possibility of logical association (linkability) with other information about the individual.
Metric	Metric is a numeric indicator(s) used to monitor and measure accomplishment of goals by quantifying the level of implementation and effectiveness. (Source: SP 800-137)
Misconfiguration	An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities. (Source: SP 800-128)
Mission-Critical System	A Mission-Critical System is a system, product or service whose failure or malfunction will result in not achieving organizational goals and objectives. Criteria are a) contains confidential or sensitive data (i.e. personally identifiable information (PII) and other regulated information), or b) serves a critical and necessary function for daily operations, or c) a combination of both protected data and critical function.
Monitoring	Monitoring is observing and checking for a set standard or configuration. Continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected. (Source: SP 800-160)
Obscured Data/Information	Data/information that has been distorted by cryptographic or other means to hide information (aka masked, obfuscated).
Operations Security	Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of planning and execution of sensitive activities.

Performance Goals	Performance Goal is the desired result(s) of implementing the security objective or technique that are measured by the metric.
Performance Measures	Performance Measures are the actions required to accomplish the performance goal validated through the completion and analysis of the institution report.
Personal Health Information (PHI)	Under the US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.
Personally Identifiable Information	<p>Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. (Source: OMB Memorandum M-07-1616)</p> <p>Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). (Source: SP 800-53 Rev. 4)</p> <p>Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (source: OMB Circular A-130)</p>
Policy	Statements, rules or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component. (Source: SP 800-95)
Principle of Least Privilege	The Principle of Least Privilege (PoLP) describes minimal user profile or access privileges to information resources based on allowing access to only what is necessary for the users to successfully perform their job requirements. (Source: SP 800-179)
Privacy Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses data or (2) an authorized user accesses data for an other-than authorized purpose. (OMB M-17-12)
Privacy Risk	The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur. (NIST PF)

Privacy Risk Assessment	A risk management sub-process specifically for identifying and evaluating privacy risk concerns.
Prior Approval	A process by which all users must gain approval prior to working with, utilizing, or implementing a process or procedure.
Problematic Data Actions	A data action that could cause an adverse effect for individuals.
Program	A group of related projects (and services) managed in a coordinated way to obtain benefits and control not available from managing them individually.
Project	A temporary endeavor undertaken to create a unique product, service, or result.
Project Risk	An uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives.
Provisioning	The process of preparing systems/products/services to permit and provide for new services to its end-users.
Public Data/Information	Data elements that have no access restrictions and are available to the general public. Also, can be designated as unrestricted data.
Reconnaissance	Activity that attempts to gather information about information systems and network architecture and activity.
Risk Management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (FIPS 200)
Risk Tolerance	The level of risk or degree of uncertainty that is acceptable to organizations. (NIST SP 800-39)
Safeguards	The protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. (Source: FIPS 200)
Schedule	The planned dates for performing schedule activities and the planned dates for meeting the schedule milestones.

Scope	The work that needs to be accomplished to deliver a product, service, or result with the specified features and functions.
Sensitive Data/Information	Data for which users must obtain specific authorization to access, since the data's unauthorized disclosure, alteration or destruction will cause perceivable damage to the USG organization. Example: personally identifiable information, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA) data, or data exempt from the Georgia Open Records Act. (Source: SP 800-53 Rev. 4)
Spam	Irrelevant or inappropriate messages sent on the Internet to a large number of recipients. The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (Source: SP 800-53 Rev. 4)
Spillage	Cybersecurity incident that resulted in the transfer of protected information (classified or CUI) onto an information system or directly to a person not authorized as the recipient. (Source: CNSSI-4009)
Split DNS	An architectural design which provides selective answers based upon a predefined condition. For example, a split DNS arrangement might supply private network answers to private users while providing different answers to public users. Internal hosts are directed to an internal domain name server for name resolution, while external hosts are directed to an external domain name server for name resolution
Standard	A standard is a requirement that: 1) supports a policy; and 2) provides for common and repeatable use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. (Source: NISTIR 8074 Vol. 2)
Suspicious Activity	Anomalous activity that requires further investigation.
System or Application Event	Activity that occurs in the operation system or in a software application, which may or may not require action.
System Owner	Person or organization having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system. (Source: SP 800-161)
Traceable	Information that is sufficient to decide about a specific aspect of an individual's activities or status.

Training	Activity involving learning or accessing knowledgebases or resources to improve a skill or behavior.
Transition Period	A period of time whereby an object moves from one state or level to another.
Truncated Alert	An event that was shortened.
Users or End Users	Users are individuals who use the information processed by an information system. (Source: FIPS 200)
Worm	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. (Source: SP 800-82 Rev. 2)

Appendix C: Acronyms (Common Abbreviations)

AUP	Appropriate Use Policy
AVC	Associate/Assistant Vice Chancellor
BCP	Business Continuity Plan
BOR	Board of Regents
BPM	Business Procedures Manual
BYOD	Bring Your Own Device
CFAA	Computer Fraud and Abuse Act
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
CPR	Cybersecurity Program Review
CR	Change Request
CSIRT	Cybersecurity Incident Response Team
DNS	Domain Name Service
DRP	Disaster Recovery Plan
ECPA	Electronic Communication Privacy Act
ERM	Enterprise Risk Management
EVC	Executive Vice Chancellor
FAQ	Frequently Asked Questions
FERPA	Federal Education Rights and Privacy Act
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Modernization Act
FSA	Federal Student Aid
FTE	Full Time Equivalent
FTP	File Transport Protocol
GLBA	Gramm-Leach-Bliley Act
GPLS	Georgia Public Library Service
GSS	General Support Systems
HIPAA	Health Insurance Portability and Accountability Act
HRM	Human Resource Management
IMAP	Internet Message Access Protocol
IOC	Indicators of Compromise
IRP	Incident Response Plan
ISO	Information Security Officer
IT	Information Technology
ITIL	Information Technology Information Library
ITS	Information Technology Services
KPI	Key Performance Indicators
LMS	Learning Management Systems
NIST	National Institute of Standards and Technology
O.C.G.A.	Official Code Georgia Annotated
OLA	Operational Level Agreement
OMB	Office of Management and Budget
OPSEC	Operational Security
PHI	Personal Health Information

PII	Personal Identifiable Information
POC	Point of Contact
POLP	Principle of Least Privilege
POP	Post Office Protocol
SACSCOC	Southern Association of Colleges and Schools Commission on Colleges
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SP	Special Publication
SSC	Shared Services Center
SSN	Social Security Number
TTP	Techniques, Tactics & Procedures
U.S.C.	United States Code
USG	University System of Georgia
USO	University System Office
VC	Vice Chancellor
VP	Vice President

Index

Abuse	101, 114
Anti-malware	68
Anti-spyware	68
Anti-virus	68, 76
Asset Management	48, 60
AUP	71, 101, 102, 114
Authentication	76, 101
Availability	101
Backup	39, 40, 93, 105
BCP	114
Bring Your Own Device	93, 102, 114
Business Case	29, 102
BYOD	93, 95, 102, 114
Change Management	27, 28, 30, 97
CIO	5, 6, 13, 14, 15, 16, 18, 19, 43, 44, 45, 54, 75, 94, 96, 103, 114
CISO	6, 94, 103, 114
Confidential Data	103
Confidentiality	64, 65, 104, 114
Continuity of Operations Planning	38, 74
Controls	68, 75, 104
COOP	38, 39, 40, 74, 114
CPR	3, 39, 46, 72, 73, 74, 114
CSIRT	114
Cybersecurity	2, 6, 38, 39, 40, 46, 48, 50, 51, 61, 63, 64, 70, 72, 73, 74, 76, 100, 104, 114
Cybersecurity Incident	40, 72, 74, 104, 114
Data At Rest	105
Data In Transit	105
Data Integrity	105
Data Steward	106
Denial of Service	106
Disaster Recovery	39, 40, 41, 114

DNS.....	2, 46, 79, 80, 99, 100, 106, 112, 114
DNS Spoofing	106
Domain Name System.....	2, 46, 79, 100
DRP	39, 41, 114
Email.....	48, 84
Endpoint Security.....	48, 68, 99, 106
Endpoint Security Management	107
Endpoints	107
Event	107, 109, 112
Exploit	107
False Positive.....	107
FERPA	14, 84, 104, 112, 114
General Support System	39, 107
GLBA.....	114
Governance.....	6, 13, 14, 45, 61, 67, 74, 96
Guideline	107
HIPAA	14, 114
Incident	3, 22, 40, 46, 48, 99, 100, 108, 114
Incident Management.....	22, 48
Incident Response.....	3, 40, 46, 72, 74, 108, 114
Information Leakage	108
Information System	16, 17, 33, 34, 48, 64, 109
IRP	114
ISO	2, 32, 40, 51, 52, 54, 69, 94, 99, 108, 114
Issues.....	21, 22, 23, 109
Linkable Information.....	109
Log Management	37, 100
<i>Malware</i>	100, 108
Metric.....	109
Mission-Critical System.....	37, 66, 104, 109
Monitoring	26, 31, 109
Passwords	76, 78, 94
PHI.....	110, 114

PII	67, 71, 115
Policy	5, 6, 41, 43, 50, 53, 71, 74, 98, 101, 102, 104, 110, 114
Principle of Least Privilege	110, 115
Privacy Breach	110
Privacy Risk	110, 111
Problem Management	22
Problematic Data Actions	111
Procurement	2, 43, 44
Program	111
Project	5, 20, 24, 25, 26, 27, 28, 29, 30, 31, 109, 111
project management	15, 20, 25
Public Data	111
Reconnaissance	111
Remediation and Mitigation Tracker	3, 46, 73, 74
Required Reporting	48, 72, 73
Resource Management	18, 43, 45, 108, 114
Risk Assessment	61
Risk Management	5, 30, 31, 38, 48, 61, 63, 64, 74, 99, 114
Risk Tolerance	111
Safeguards	111
Scope	6, 27, 28, 79, 112
Security	6, 17, 48, 65, 66, 69, 70, 75, 76, 77, 94, 99, 103, 107, 115
Security Awareness, Training and Education	69, 70
Sensitive Data	112
Service Desk	21
Service Level Agreements	21, 42
Service Metrics	23
SLA	22, 23, 42, 115
Spillage	106, 112
Standard	3, 37, 38, 39, 41, 46, 48, 77, 86, 87, 88, 93, 95, 112
Suspicious Activity	82, 112
System Owner	112
Trojan	104, 108

University System of Georgia.....	2, 41, 72, 93
User Account Management	33, 34
Worm	113