Table of Contents

Introduction

Section 1.0: Information Technology (IT) Governance
   1.1 Chief Information Officer Role and Responsibilities
   1.2 Governance Structure
   1.3 IT Organization, Roles and Responsibilities and Processes
   1.4 Strategic Planning
   1.5 Resource Management

Section 2.0: Project and Service Administration
   2.1 Service Administration
   2.2 Project Administration
   2.3 Project Documentation Templates

Section 3.0: IT Management
   3.1 Information System User Account Management
   3.2 Log Management
   3.3 Continuity of Operations Planning
   3.4 Network Services

Section 4.0: Financial and Human Resource Management
   4.1 Technology Procurement Approval Process
   4.2 Financial Management
4.3 Human Resource Management

Section 5.0: Cybersecurity

5.1 USG Cybersecurity Program
5.2 Organization and Administration
5.3 Incident Management
5.4 USG Information Asset Management and Protection
5.5 Risk Management
5.6 USG Information System Categorization
5.7 USG Classification of Information
5.8 Endpoint Security
5.9 Security Awareness, Training and Education
5.10 Required Reporting
5.11 Minimum Security Standards for USG Networked Devices
5.12 Password Security
5.13 Domain Name System
5.14 Identity Theft Prevention - Red Flags Rule
5.15 Email Use and Protection

Section 6.0: ePrivacy

6.1 USG Privacy Standard
6.2 USG Web Privacy Standard

Section 7.0: Facilities

Section 8.0: Bring Your Own Device (BYOD) Standard

8.1 Purpose
8.2 Applicability
8.3 Standards
8.4 Standard Non-Compliance
Section 9.0: Data Governance and Management Structure

9.1 Purpose
9.2 Data Management Structure
9.3 Data Classification
9.4 Data Access
9.5 Privacy and Security

Section 10.0: Learning Management System (LMS)

10.1 Applicability
10.2 Service Description
10.3 Participation Model
10.4 Governance
10.5 Resource Model
# Information Technology Handbook

## IT Handbook Version Control

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Version</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/18/2016</td>
<td>Revised cost estimate</td>
<td></td>
<td>Section 4.1 - added a statement in IT Procurement Policies.</td>
</tr>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format.</td>
<td>2.0</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
<tr>
<td>05/17/2016</td>
<td>System-level password</td>
<td>2.1</td>
<td>Section 5.12.3 - added a statement about system-level passwords in bullet point number 4.</td>
</tr>
<tr>
<td></td>
<td>information added.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/27/2016</td>
<td>Updated flow chart</td>
<td>2.2</td>
<td>Section 3.1 - updated “Recommended Process Flow Chart” added to match content.</td>
</tr>
<tr>
<td>05/27/2016</td>
<td>Introduction to the IT</td>
<td>2.2</td>
<td>Section Introduction - updated entire section.</td>
</tr>
<tr>
<td></td>
<td>Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11/1/2016</td>
<td>Department title changed</td>
<td>2.3</td>
<td>As of Nov. 1, 2016 the department name changed to Cybersecurity.</td>
</tr>
<tr>
<td>11/3/2016</td>
<td>Revised Domain Name System</td>
<td>2.3</td>
<td>Section 5.13 – content in section was updated and revised.</td>
</tr>
<tr>
<td></td>
<td>Guidelines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11/3/2016</td>
<td>Domain Name System</td>
<td>2.3</td>
<td>Section 5.13 – added link to the revised Domain Name System (DNS) Guidelines.</td>
</tr>
<tr>
<td></td>
<td>Guidelines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11/3/2016</td>
<td>Addition to USG organizations</td>
<td>2.3</td>
<td>Section Introduction – Georgia Film Academy added to the list of USG organizations.</td>
</tr>
<tr>
<td>11/17/2016</td>
<td>Clarification of information system owner</td>
<td>2.4</td>
<td>Section 1.3.2 – added clarification of information system owner roles and responsibilities within the framework of people, process and technology.</td>
</tr>
<tr>
<td>11/17/2016</td>
<td>Spending limits updated</td>
<td>2.4</td>
<td>Section 4.1 – updated spending limits for purchases in excess of $1 million.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for</td>
<td>2.5</td>
<td>Section 1.2 – added the correct title to 1.2.1.</td>
</tr>
<tr>
<td></td>
<td>consistency in format and content. Added title.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for</td>
<td>2.5</td>
<td>Section 1.3 – deleted a misplaced word.</td>
</tr>
<tr>
<td></td>
<td>consistency in format and content.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Name</td>
<td>Version</td>
<td>Description of Change</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format and content. Changed location of definitions.</td>
<td>2.5</td>
<td>Section 3.0 – added definitions from 3.1 and deleted definitions already stated in Introduction section.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format and content. Changed location of definitions.</td>
<td>2.5</td>
<td>Section 3.1 – moved definitions to 3.0.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format and content. Deleted exceptions.</td>
<td>2.5</td>
<td>Section 3.2 – deleted exceptions to log management standard.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format and content. Added accurate titles and deleted standard.</td>
<td>2.5</td>
<td>Section 3.3 – provided accurate title for ISO and deleted management of USG continuity of operations planning standard.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format and content. Deleted table.</td>
<td>2.5</td>
<td>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.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format and content.</td>
<td>2.5</td>
<td>Section 5.10 – added content for clarification.</td>
</tr>
<tr>
<td>09/07/2017</td>
<td>Reviewed and revised entire Section 5 for consistency of content</td>
<td>2.6</td>
<td>Section 5 - Added “USG organizations” as stated in the Introduction section and other minor editorial changes removing policy and standard where appropriate.</td>
</tr>
<tr>
<td>09/07/2017</td>
<td>Incorporated revisions in Section 5 by University of North Georgia</td>
<td>2.7</td>
<td>Section 5 - Incorporated minor editorial changes recommended by University of North Georgia.</td>
</tr>
<tr>
<td>01/02/2019</td>
<td>Revised Section 5.10 to align with the NIST framework and FIPS.</td>
<td>2.8</td>
<td>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. Table of Contents added.</td>
</tr>
</tbody>
</table>
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 handbook respects the value of the diversity of USG organizations while providing guidance with regards to information technology (IT) operations within the USG.

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 (VC/CIO), under Board of Regents (BOR) Policy 11.1.1, 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 handbook of Information Technology (IT) standards and best practices to be followed by USG organizations.

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

1. BOR Policy Manual is the top-level set of Board approved policies from which all lower-level USG documents flow. Section 7.14 covers Identity Theft and Section 7.15 describes the Risk Management Policy including objectives and oversight. Compliance Policy is covered in Section 7.16 and defines applicability and implementation. Section 11.0, Information Technology, covers all aspects of USG information technology including general policy, IT project authorization and information security.

2. USG IT Handbook is a standard containing the IT requirements and recommendations that establish acceptable IT practices for USG organizations.

3. USG Organization Policies and Procedures establish the detailed practices and tools used by USG organizations to meet the standards set forth in the USG IT Handbook.

4. Program or Project Policies and Procedures establish the detailed practices and tools to implement the standards and best practices set forth in the USG IT Handbook or USG organizations’ policies and procedures.

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 and state of Georgia, BOR policy mandates, and IT 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 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 IT Handbook, while focusing on USG standards, also offers ready access to important policies, statutes and regulations that will aid the IT officer in his or her daily performance of duties.
Governance, Compliance and Authority

The USG chief information officer 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 the BOR Policy Manual §§ 7.14 - 16, and 11.1 - 3 as well as the USG's Appropriate Usage Policy.

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

Scope

This standard applies to USG organizations.

Implementation and Applicability

A systemwide approach to IT operations and cybersecurity compliance shall be adopted by USG organizations. It is expected that cybersecurity processes 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 develop the origination’s cybersecurity plans, standards and guidelines to:

- Identify and document applicable policies, procedures, laws and regulations.
- Establish the roles and responsibilities necessary to manage a cybersecurity program.
- Appoint skilled personnel into the identified roles.
- Communicate the importance of polices, standards and guidelines as defined in BOR Policy Manual 11.3.3.
- Submit annually the Information Security Program Review as defined by BOR Policy Manual 11.3.3.

Exceptions

Exceptions to any policy, standard, process, procedure or guideline set forth in the IT Handbook shall be at the discretion of, and approved in writing by, the USG VC/CIO or the USG Chief Information Security Officer (CISO). In each case, USG organizations or vendors must complete and submit an Information Security Policy 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. Denials of requests for exceptions may be appealed to the USG VC/CIO or CISO.

Definitions

The following definitions of Shall, Will, Must, May, May Not, and Should are used throughout this 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

Section 1.0: Information Technology (IT) Governance
Section 2.0: Project and Service Administration
Section 3.0: IT Management
Section 4.0: Financial and Human Resource Management
Section 5.0: Cybersecurity
Section 6.0: ePrivacy
Section 7.0: Facilities
Section 8.0: Bring Your Own Device (BYOD) Standard
Section 9.0: Data Governance and Management Structure
Section 10.0: Learning Management System (LMS)
Information Technology (IT) Governance

Section Control

Revision History

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

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Service Administration</td>
<td>July 2015</td>
<td>July 2015</td>
<td>December 2015</td>
</tr>
</tbody>
</table>
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 two essential elements that should be formally prescribed are:

- A well-defined and understood role for the organization’s Chief Information Officer (CIO).
- A well-defined and adopted working relationship between the CIO and the other Chief Officers (CxOs) also known as a governance structure.
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.
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 (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.

**Shared Governance Framework** 1.2.1

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 with regard to 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.

**Strategic Alignment** 1.2.2

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.
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.

**Organization**

**1.3.1 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, as long as 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 any and 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.
IT System Ownership Roles and Responsibilities 1.3.2

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 employed by USG organizations requires strong collaboration between three primary audiences: information system owners, operation and security 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 is normally the information system owner. However, the designation is dependent upon the organizational structure.

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. 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, 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 security requirements.

- Technology

  - Establish through contract, statement of work, memorandum of understanding, or service level agreement, the technology responsibilities of IT in support of the information system or services.

  - Provide liaison between the IT service unit and the customers served by the information system or services provided by IT.

In support of the information system owner, Information Security Officers are responsible for managing the repository of inventoried information systems, 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 Business Procedures Manual, 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 Information Security Officer 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.

People, Process and Technology Framework
References

- NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-65, Revision 1 (Draft), Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (Draft), Section 2.6.2.11 System Owner
Strategic Planning

The 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.

Technology Direction Planning 1.4.1

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.

Standards and Quality Practices 1.4.2

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.

Development and Acquisition Standards 1.4.3

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.
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 in order to enable planning and avoid unexpected issues. The CIO should adjust the planning for performance and capacity following analysis of these measures.
## Section Control

### Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
</tbody>
</table>

### Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

IT service can be defined as a set of related functions provided by IT systems 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 a number of 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 planning, 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.

Definitions

The following definitions of Program, Project, Scope, Risk, Issues, Schedule, and Business Case are used throughout this section:

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.

Scope: The work that needs to be accomplished to deliver a product, service, or result with the specified features and functions.

Risk: An uncertain event or condition that, if it occurs, has a positive or negative effect on a project’s objectives.

Issues: A problem impacting the successful outcome of a project. Project issues should be tracked through resolution.
Schedule: The planned dates for performing schedule activities and the planned dates for meeting the schedule milestones.

Business Case: A description of a requested project or initiative that explains the goals, benefits, and cost of the request.
Service Administration

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 taken into account.

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 as 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 in order 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 as a result 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.

In the event that 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 institution or organization, but also on a system-wide 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 institution 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 in order 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 in order 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 in order to close the gap to best practice.
- Setting up an implementation plan.
- Controlling results and improvements.
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:

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.
7. Risk management approach.
8. Testing and implementation.

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 methodology 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.


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 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.

### Planning 2.2.2

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 so as 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. Refer to Section 6.0, Risk Management, of this Handbook for more information.

### Execution 2.2.3

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.

### Monitoring and Controlling 2.2.4

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.

### Closing 2.2.5

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.
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.

**Project Scope**

The project scope document must include project goals and deliverables.

<table>
<thead>
<tr>
<th>Project Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project Sponsor</th>
<th>IT Project Sponsor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program Manager</th>
<th>Project Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Executive Summary</th>
<th>High level description of the project, linkages to strategic goals, and justification.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Description</td>
<td>Who, what, when and why of the project.</td>
</tr>
<tr>
<td>Project Goals and Objectives</td>
<td>These may come from the business case, but should be refined if additional information is available.</td>
</tr>
<tr>
<td>Project Scope</td>
<td>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.</td>
</tr>
<tr>
<td>Project Deliverables</td>
<td>What will be produced as a result of this project.</td>
</tr>
<tr>
<td>Assumptions and Constraints/Boundaries</td>
<td>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.</td>
</tr>
<tr>
<td>Project Dependencies</td>
<td>Conditions that must exist or be met in order for the project to move forward and successfully meet its objectives.</td>
</tr>
</tbody>
</table>

Signature

______________________________________  __________________________
Project Sponsor                                                Date
**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.

### Change Management Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project manager</td>
<td>• Develop change management plan</td>
</tr>
<tr>
<td></td>
<td>• Take change requests to change review board</td>
</tr>
<tr>
<td></td>
<td>• Monitor change requests</td>
</tr>
<tr>
<td></td>
<td>• Log change requests</td>
</tr>
<tr>
<td>Project team</td>
<td>• Evaluate change requests and estimate impact to scope, schedule, and budget</td>
</tr>
<tr>
<td>Role</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change Review Board</td>
<td>• Evaluate change requests and making decisions as to whether they are accepted, rejected, or deferred</td>
</tr>
<tr>
<td>Sponsors (Project/IT)</td>
<td>• Approve change management plan</td>
</tr>
</tbody>
</table>

### Change Review Board

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project manager</td>
<td></td>
</tr>
<tr>
<td>Change Review Board leader</td>
<td></td>
</tr>
<tr>
<td>Technical Review Board members</td>
<td></td>
</tr>
<tr>
<td>Change Review Board members</td>
<td></td>
</tr>
</tbody>
</table>

### Change Control Documents

<table>
<thead>
<tr>
<th>Document</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change request</td>
<td>• Documents desired changes as requested or discovered</td>
</tr>
<tr>
<td></td>
<td>• Documents what the change is</td>
</tr>
<tr>
<td></td>
<td>• Documents the rationale and benefit of the change</td>
</tr>
<tr>
<td></td>
<td>• Documents the risk of not changing</td>
</tr>
<tr>
<td>Change/Decision log</td>
<td>• Summarizes change requests received</td>
</tr>
<tr>
<td></td>
<td>• Tracks status of change requests submitted</td>
</tr>
<tr>
<td></td>
<td>• Documents change decisions made, when, and by whom</td>
</tr>
<tr>
<td>Type of Change</td>
<td>Control Document</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| Scope         | • Scope statement  
               • WBS (work breakdown structure)  
               • Product requirements  
               • Scope management plan |
| Time          | • Schedule baseline  
               • Schedule  
               • Milestones  
               • Schedule management plan |
| Costs         | • Cost baseline  
               • Budget  
               • Cost management plan |
| Risk          | • Risk management matrix  
               • Risk management plan |
| Communications| • Communication plan  
               • Stakeholder analysis |
| Resources     | • 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:

| 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:

| 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 Change Request 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.

Risk Management Plan

Purpose

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.

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager</td>
<td>• Leads the development of a project Risk Management Plan&lt;br&gt;• Leads the project team through identification of risks&lt;br&gt;• Facilitates risk analysis with Risk Management Team&lt;br&gt;• Monitors and escalates risks to the Risk Management Lead</td>
</tr>
<tr>
<td>Role</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Project Sponsor</td>
<td>• Approves the Risk Management Plan</td>
</tr>
<tr>
<td>Risk Management Lead</td>
<td>• Chairs the Risk Management Team</td>
</tr>
<tr>
<td></td>
<td>• Approves Risk Scoring</td>
</tr>
<tr>
<td></td>
<td>• Approves risk disposition strategy</td>
</tr>
<tr>
<td>Risk Management Team</td>
<td>• Identifies risks</td>
</tr>
<tr>
<td></td>
<td>• Conducts risk impact analysis</td>
</tr>
<tr>
<td></td>
<td>• Develops disposition strategy recommendations</td>
</tr>
<tr>
<td>Project Team</td>
<td>• Identifies risks</td>
</tr>
</tbody>
</table>

**Risk Management Methodology**

**Risk Identification**

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.

**Risk Qualification/ Quantification**

In order 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>
<thead>
<tr>
<th>Probability</th>
<th>Impact</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>75% - 100%</td>
<td>Critical: Project stops or fails</td>
<td></td>
</tr>
<tr>
<td>51% - 74%</td>
<td>Elevated: Major impact to project timeline, costs, or scope</td>
<td></td>
</tr>
</tbody>
</table>
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 in order 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 so as 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>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Timeline</th>
<th>Probability</th>
<th>Impact</th>
<th>Score</th>
<th>Risk Exposure</th>
<th>Risk Status</th>
<th>Disposition</th>
<th>Trigger Date</th>
<th>Action Description</th>
<th>Owner</th>
<th>Updated Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
<td>Timeline</td>
<td>Probability</td>
<td>Impact</td>
<td>Score</td>
<td>Risk Exposure</td>
<td>Risk Status</td>
<td>Disposition</td>
<td>Trigger Date</td>
<td>Action Description</td>
<td>Owner</td>
<td>Updated Date</td>
</tr>
<tr>
<td>----</td>
<td>-------------</td>
<td>----------</td>
<td>-------------</td>
<td>--------</td>
<td>-------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>-------</td>
<td>--------------</td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 Control

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
<tr>
<td>05/27/2016</td>
<td>Updated flow chart</td>
<td>Section 3.1 - updated “Recommended Process Flow Chart” added to match content.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format</td>
<td>Section 3.0 – added definitions from 3.1 and deleted definitions already stated in</td>
</tr>
<tr>
<td></td>
<td>and content. Changed location of definitions.</td>
<td>Introduction section. Section 3.1 – moved definitions to 3.0.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format</td>
<td>Section 3.2 – deleted exceptions to log management standard.</td>
</tr>
<tr>
<td></td>
<td>and content. Deleted exceptions.</td>
<td></td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format</td>
<td>Section 3.3 – provided accurate title for ISO and deleted management of USG continuity</td>
</tr>
<tr>
<td></td>
<td>and content. Added accurate titles and</td>
<td>of operations planning standard.</td>
</tr>
<tr>
<td></td>
<td>deleted standard.</td>
<td></td>
</tr>
</tbody>
</table>

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Information System User Account Management</td>
<td>November 2012</td>
<td>March 2013</td>
<td>July 2013</td>
</tr>
</tbody>
</table>
Introduction

Knowledge Management provides information technology 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 both at the System and institution levels. 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.

Definitions

The following definitions of Critical System, Principle of Least Privilege (PoLP), Sensitive Information, System Owner, and Users are used throughout this section.

1. A Critical System is a system whose failure or malfunction will result in not achieving organization goals and objectives.

2. Confidential and Sensitive information is defined in section 5.7 of the IT Handbook.

3. Data Steward is defined in section 9.2 of the IT Handbook. Examples are the registrar and director of human resources (HR).

4. Human Resource Management (HRM) is the area of administrative focus pertaining to an organization's employees. HRM is sometimes referred to simply as HR.

5. Information System is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

6. 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.

7. Sensitive Information is information maintained by USG organizations that requires special precautions, as determined by institution standards and risk management decisions, to ensure its accuracy and integrity by using integrity, verification, and access controls to protect it from unauthorized modification or deletions.

8. A System Owner is the manager or agent responsible for the function that is supported by the resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The system owner is responsible for establishing the controls that provide the security. The system owner of a collection of information is the person responsible for the business results of that system or the business use of the information.

9. Users are individuals who use the information processed by an information system.
Information System User Account Management

Introduction

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.

Information System User Account Management 3.1.1

Controlling access to information systems 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 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, reviewed and deactivated 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 in order to lower the risks and threats facing users, hosts, networks and business operations.

Information System User Account Management Procedures 3.1.1.1

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 must be protected from unauthorized access, loss, contamination or destruction. Proper management and protection is 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 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.
Procedures

-USG organizations shall identify and categorize information systems that process or store confidential or sensitive information, or are critical systems. The suggested responsible party is the system owner.

-USG organizations will identify the system owner and data steward for each critical system or systems containing confidential or sensitive information. A list of these systems 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. 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.

-USG organizations will define both administrative and technical access controls. 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.

-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 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.
Recommended Process Flow Chart

- Employee’s manager and/or data steward determine access needed to perform duties.
- System owner awards access.
- System owner provides list of users with system access and access details/roles to respective data stewards.
- Data stewards validate that access is appropriate.
- Validation process is documented for use by management or outside auditors.

- Employee’s manager notifies HR.
- HR notifies system owners and data stewards.
- System owner terminates or updates access as appropriate.
- Employee’s manager and/or data steward determine access needed to perform new duties.
- HR notifies system owner and data stewards.
- System owner removes access no longer needed and adds access required by new responsibilities.

References

- Special Publication 800-53, Revision 4, *Security and Privacy Controls for Information Security Systems*
- Federal Information Policy, 44 U.S.C, Sec 3502 (8)
Log Management

Section 3.2

Purpose 3.2.1

Logs contain information related to many different types of events occurring within systems, 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. The dominant problem with log management is ensuring that security, system and network administrators regularly perform effective analysis of log data.

Objective 3.2.2

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

- Proactive maintenance of information system resources.
- Awareness of “normal” vs. “abnormal” network traffic or system performance.
- Support after-the-fact investigations of security incidents.

Standard 3.2.3

USG resources that store, access or transmit data and categorized as “HIGH” 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.

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.
## Log Retention and Analysis Frequency

<table>
<thead>
<tr>
<th>Category</th>
<th>Low Impact Systems</th>
<th>Moderate Impact Systems</th>
<th>High Impact Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log retention</td>
<td>1 to 2 weeks</td>
<td>1 to 3 months</td>
<td>3 to 12 months</td>
</tr>
<tr>
<td>How often log data needs to be analyzed (through automated or manual means)</td>
<td>Every 1 to 7 days</td>
<td>Every 1 to 3 days</td>
<td>Once a day</td>
</tr>
</tbody>
</table>

### References and Resources

3.2.4

- [NIST SP800-92 Guide to Computer Security Log Management](#).
- [IT Handbook Section 5.6 USG Information System](#).
- [Categorization Standard USG Records Retention Schedule](#).
USG Continuity of Operations Planning Standard  3.3.1  

Purpose

Continuity of Operations Planning (COOP), 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. COOP is an effort to ensure that at minimum, the general support system (GSS) continues to operate and be available.

Scope, Enforcement, Authority

- BOR Policy Manual, Section 11.0
- USG Office of Information Security Program Policy
- USG IT/IS Risk Management Standard
- USG Information Security Program Reporting Policy

Guiding Principles


- The USG Continuity of Operations Plan will require the involvement of all USG organizations to ensure an effective University System response to contingencies and disasters.

- The USG Continuity of Operations Plan must incorporate the physical and logistical limitations of the USG operating locations.

- The USG Continuity of Operations Plan will be aligned with and operationalize the USG Emergency Operations Plan and the Enterprise Risk Management Program.

Standard

Recovery strategies must be developed for information technology (IT) systems. 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.

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 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 general support system 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

Backup and retention schedules and procedures are critical to the recovery of USG organization's systems, applications 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 are capable of developing 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 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. 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.

-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 in order 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/Business Recovery Plan.
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 and technology, and to all users of these resources, systems and technology within the USG information infrastructure. Compliance with this standard is mandatory.

Resources

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- ISO 27005 Information Security Risk Management (ISRM)
- NIST Special Publication 800-30 (Risk Management)
- NIST SP 800-34, Revision 1 – Contingency Planning Guide for Federal Information Systems
- USG Continuity of Operations Planning Template and Guide
Network Services Standard

3.4.1 Purpose

PeachNet®, the University System of Georgia’s (USG) 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 Board of Regents of the University System of Georgia’s 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 (CoLo) 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.
Financial and Human Resource Management

Section Control

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/18/2016</td>
<td>Revised cost estimate</td>
<td>Section 4.1 - added a statement to the IT Procurement Policies.</td>
</tr>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
<tr>
<td>11/17/2016</td>
<td>Spending limits updated</td>
<td>Section 4.1 – updated spending limits for purchases in excess of $1 million.</td>
</tr>
</tbody>
</table>

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Sound management principles are required for the budget and human resources allocated to the Chief Information Officer (CIO) and centralized Information Technology (IT) organization. In the event any standards defined in this Handbook are in conflict with the University System of Georgia (USG) Board of Regents (BOR) policy or procedures as defined in other relevant guides such as the Fiscal Affairs Business Procedures Manual (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.
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 Vice Chancellor and Chief Information Officer (VC/CIO).

Section 11.2 of the BOR Policy Manual (BPM) delegates authority from the BOR to the USG VC/CIO to approve USG technology procurements on their behalf. Section 11.2.1 authorizes the USG VC/CIO to further delegate approval authority to institution presidents or their designee(s). This section of the USG IT Handbook implements this BOR policy.

Spending Limits

4.1.1

The USG VC/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 and the University of Georgia.

2. $250,000: Columbus State University, University of North Georgia, Georgia Southern University, Kennesaw State University, University of West Georgia and Valdosta State University.

3. $100,000: All other USG organizations.

IT Procurement Policies

4.1.2

1. Information Technology is defined in Section 11.0, Information Technology (IT), 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 VC/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 VC/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 VC/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 VC/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.

**Requesting Approval**

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

Section Control

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
<tr>
<td>05/17/2016</td>
<td>System-level password information added.</td>
<td>Section 5.12.3 - added a statement about system-level passwords in bullet number 4.</td>
</tr>
<tr>
<td>11/3/2016</td>
<td>Revised Domain Name System</td>
<td>Section 5.13 – content in section was updated and revised.</td>
</tr>
<tr>
<td>11/3/2016</td>
<td>Domain Name System Guidelines</td>
<td>Section 5.13 – added link to the revised Domain Name System (DNS) Guidelines.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format and content. Deleted table.</td>
<td>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.</td>
</tr>
<tr>
<td>05/15/2017</td>
<td>Revised section for consistency in format and content.</td>
<td>Section 5.10 - added content for clarification.</td>
</tr>
<tr>
<td>09/07/2017</td>
<td>Reviewed and revised entire Section 5 for consistency of content</td>
<td>Section 5 - added “USG organizations” as stated in the Introduction section and other minor editorial changes removing policy and standard where appropriate.</td>
</tr>
<tr>
<td>09/07/2017</td>
<td>Incorporated revisions in Section 5 by University of North Georgia</td>
<td>Section 5 - Incorporated minor editorial changes recommended by University of North Georgia.</td>
</tr>
<tr>
<td>1/2/2019</td>
<td>Revised Section 5.10 to align with the NIST framework and FIPS.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
</table>
Definitions

The following definitions of shall, will, must, may, may not, and should are used throughout this Handbook.

1. Shall, Will, and Must indicate a legal, regulatory, standard, or policy requirement. Shall and Will are used for persons and organizations, and Must 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. The focus of should statements generally is more outcome-based; i.e., an alternate method to achieve the requirement may be developed assuming it is documented as effectively managing risk.


1. Authentication is a process of attempting to verify the digital identity of a system user or processes.
2. Availability ensures timely and reliable access to and use of information.
3. Confidentiality preserves authorized restrictions on information access and disclosure, and includes means for protecting personal privacy and proprietary information.
4. Computer Security Incident is a violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices, which may include, but are not limited to:
   - Widespread infections from virus, worms, Trojan horse or other malicious code;
   - Unauthorized use of computer accounts and computer systems;
   - Unauthorized, intentional or inadvertent disclosure or modification of sensitive/critical data or infrastructure;
   - Intentional disruption of critical system functionality;
   - Intentional or inadvertent penetration of firewall;
   - Compromise of any server, including Web server defacement or database server;
   - Exploitation of other weaknesses, known or unknown;
   - Child pornography;
   - Attempts to obtain information to commit fraud or otherwise prevent critical operations or cause danger to state or system or national security and
   - Violations of state or USG security policies or standards that threaten or compromise the security objectives of state or USG data, technology, or communications systems; and,
   - Any violation of the “Appropriate Use Policy.”
5. DNS refers to the domain name system, which represents a powerful Internet technology for converting domain names to their corresponding IP addresses.
6. DNS Spoofing refers to confusing a DNS server into giving out bad information.
7. Domain is most often used to refer to a domain zone; it is also used to describe a zone or a domain name.

8. 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.

9. 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.

10. 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.

11. 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.

12. Event of Interest is 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.

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

14. Incident Management is the process of detecting, mitigating, and analyzing threats or violations of security policies and controls and limiting their effect.

15. Incident Response Management is the process of detecting, mitigating, and analyzing threats or violations of security policies and limiting their effect.

16. Integrity is the accuracy and reliability of the information and system against unauthorized modification.

17. Metric is a numeric indicator(s) used to monitor and measure accomplishment of goals by quantifying the level of implementation and effectiveness.

18. Monitoring is observing and checking for a set standard or configuration.

19. Performance Goal is the desired result(s) of implementing the security objective or technique that are measured by the metric.

20. Performance Measures are the actions required to accomplish the performance goal validated through the completion and analysis of the institution report.

21. Policies typically are concise documents that outlines specific requirements, business rules, or position that must be met.

22. Safeguards are proactive measures prescribed to meet the security requirements specified for an information system.

23. Split DNS is when 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.
24. A standard is a requirement that supports a policy.

## Implementation and Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
<th>Revision Date(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>USG Cybersecurity Program</td>
<td>February 2009</td>
<td>February 2009 to Cybersecurity</td>
<td>February 2009</td>
<td>May 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>February 2013 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.2</td>
<td>Cybersecurity Organization and Administration</td>
<td>February 2009</td>
<td>February 2009 to Cybersecurity</td>
<td>February 2009</td>
<td>May 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>February 2013 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.3</td>
<td>Incident Management</td>
<td>December 2008</td>
<td>December 2008 to Cybersecurity</td>
<td>February 2009</td>
<td>May 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>February 2013 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.4</td>
<td>USG Information Asset Management and Protection</td>
<td>July 2013</td>
<td>May 2014</td>
<td>TBD</td>
<td>May 2014</td>
</tr>
<tr>
<td>5.5</td>
<td>IT/IS Risk Management</td>
<td>April 2010</td>
<td>April 2010 to Cybersecurity</td>
<td>April 2010</td>
<td>May 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>February 2013 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>USG Information System Categorization</td>
<td>June 2013</td>
<td>May 2014</td>
<td>July 2014</td>
<td>May 2014</td>
</tr>
<tr>
<td>5.7</td>
<td>USG Classification of Information</td>
<td>June 2013</td>
<td>May 2014</td>
<td>July 2015</td>
<td>May 2014</td>
</tr>
<tr>
<td>5.8</td>
<td>USG Endpoint Security</td>
<td>June 2013</td>
<td>May 2014</td>
<td>July 2015</td>
<td>May 2014</td>
</tr>
<tr>
<td>5.9</td>
<td>Security Awareness, Training, and Education</td>
<td>April 2009</td>
<td>April 2009 to Cybersecurity</td>
<td>April 2009</td>
<td>May 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>February 2013 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.10</td>
<td>Required Reporting</td>
<td>April 2009</td>
<td>April 2009 to Cybersecurity</td>
<td>April 2009</td>
<td>May 2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>February 2013 to IT Handbook</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Information and information systems are strategic assets of the University System of Georgia (USG). The Board of Regents (BOR) recognizes that information created, collected, or distributed using technology by any USG organization is a valuable asset and must be protected from unauthorized disclosure, modification, or destruction. The degree of protection needed is based on the nature of the resource and its intended use. USG organizations have the responsibility to employ prudent cybersecurity standards and best practices to minimize the risk and threats to the integrity, confidentiality, and availability of USG information and information systems.

Cybersecurity means the protection of information and information systems, equipment, and people from a wide spectrum of risks and threats. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information, regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction.

It is USG policy to provide an environment that encourages the free exchange of ideas and sharing of information. Access to this environment and the USG’s information technology (IT) resources is a privilege and must be treated with the highest of ethical standards.
Applicability

USG organizations must comply with the cybersecurity and privacy policies, standards, and procedures issued by USG Cybersecurity, and report and file the appropriate compliance documents. USG organizations must adhere to the Cybersecurity Reporting Requirements, as noted in Section 5.10 of this Handbook.

The scope of this section is to have broad application, particularly with respect to information and information systems, which affect the operational levels of USG organizations. In a similar manner, all contractual agreements with 3rd party vendors must adhere to the guidance provided. An appropriate Service Level Agreement (SLA) and Non-Disclosure Agreement (NDA) should be constructed to ensure roles and requirements are acknowledged and followed.
Section 11.3 of the BOR Policy Manual charges USG Cybersecurity within Information Technology Services (ITS) with the responsibility and authority to:

1. Create, issue, and maintain cybersecurity standards and guidelines.
2. Direct USG organizations to effectively manage security, privacy and risk.
3. Advise and consult with USG organizations on cybersecurity issues.
4. Attest USG institutions are in compliance with the requirements specified in the BOR Policy Manual, local laws, state law, federal laws, codes and regulations.

Based on this direction, the USG Chief Information Security Officer (CISO) shall develop and maintain a cybersecurity organization and architecture for support of cybersecurity across the USG and support of activities between USG organizations. The CISO shall maintain cybersecurity standards and guidelines that the USG organizations must consider in the development of their individual cybersecurity plans.

The USG CISO will:

1. Assess performance, returning value while managing risk.
2. Assume and accept responsibility for the charge given and resources received.
3. Align the interests of different entities.
4. Lead USG cybersecurity and privacy efforts.
5. Measure results.
6. Implement continuous improvement.

### USG Organizational Responsibilities 5.1.1

USG organizations must provide for the proper use and protection of its information assets. Accordingly, USG organizations must:

1. Build a cybersecurity program;
2. Assign management responsibilities for cybersecurity program, including the appointment of an Information Security Officer (ISO), as noted in Section 5.2 of this Handbook;
3. Develop and maintain a computer/data incident management component as noted in Section 5.3 of this Handbook;
4. Develop and maintain a program to manage and protect information assets, as noted in Section 5.4 of this Handbook;
5. Establish and maintain an information technology and cybersecurity risk management program, including a risk assessment, analysis, planning mitigation, and monitoring process as noted in Section 5.5 of this Handbook;
6. Categorize information systems, as noted in Section 5.6 of this Handbook;
7. Classify information records (data), as noted in Section 5.7 of this Handbook;

8. Implement the minimum endpoint security standard requirements/capabilities, as noted in Section 5.8 of this Handbook;

9. Maintain an annual cybersecurity awareness, and training component for all employees and contractors, as noted in Section 5.9 of this Handbook;

10. Comply with USG reporting requirements, as noted in Section 5.10 of this Handbook, including developing and maintaining a cybersecurity and privacy policy and compliance management process, and building, testing, and maintaining a Continuity of Operations Plan (C.O.O.P.) including a:
   - Backup and Recovery Plan
   - Incident Management Plan
   - Note: It is our future intention to require that the C.O.O.P. include a Disaster Recovery Plan and a Business Continuity Plan.

11. Implement minimum security standards for networked devices, as noted in Section 5.11 of this Handbook;

12. Implement password security controls, as noted in Section 5.12 of this Handbook;

13. Implement and administer domain name security, as noted in Section 5.13 of this Handbook;

14. Make reasonable efforts to detect, prevent, and mitigate identity theft, as noted in Section 5.15 of this Handbook.

15. Implement the standard for the appropriate use and protection of USG email systems, as noted in Section 5.16 of this Handbook.

**Policy, Standards, Processes, and Procedure Management Requirements**

5.1.2

The purpose of this section is to establish and maintain a “standard of due care” to prevent misuse or loss of USG information assets. Policy provides management direction for USG organizations to conform to business requirements, laws, and administrative policies. Standards are the specifications that contain measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy. Procedures are the specific series of actions that are taken in order to comply with policies and standards.

USG organizations must provide for the integrity and security of its information assets by creating appropriate internal policies, processes, standards, and procedures for preserving the integrity and security of each automated, paper file, or database. 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. Establish appropriate academic and administrative policies, processes, and procedures to protect and secure IT infrastructure, including:

- 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.

- 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.

- Intrusion Prevent System (IPS)/firewall configurations, which must require creation and documentation of a baseline configuration for each IPS/firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.

- 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, 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.

- 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. Further, this must address, and be consistent with, the organization’s policy for making security upgrades and security patches.

- 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.

- 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.

5. 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 security, which have been established for the original data file, must be applied in the new environment.

6. Establish policy requiring encryption, or equally effective measures, for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs, DVDs, and thumb drives) and on portable computing devices (including, but not limited to, state assets: mobile devices, tablets, and laptop and notebook computers).

**USG Appropriate Use Policy (AUP) Guidelines**

This section establishes a USG-wide guideline regarding developing an appropriate use policy of USG information technology (IT) resources.
It is USG policy to provide an environment that encourages the free exchange of ideas and sharing of information. Access to this environment and the USG’s IT resources is a privilege and must be treated with the highest standard of ethics.

The USG expects all organizations and their users to use IT resources in a responsible manner, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and federal laws, and USG policies and standards. USG organizations may develop policies, standards, and guidelines based on their specific needs that supplement, but do not lessen, the intent of this policy.

This guideline outlines the standards for appropriate use of USG IT resources, which include, but are not limited to, equipment, software, networks, data, and telephones whether owned, leased, or otherwise provided by USG organizations. This guideline applies to all users of USG IT resources including faculty, staff, students, guests, external organizations and individuals accessing network services, such as the Internet via USG resources.

Guidelines

Preserving the access to information resources is a system-wide effort that requires each institution to act responsibly and guard against abuses. Therefore, USG organizations and its users have an obligation to abide by the following standards of appropriate and ethical use:

- Use only those IT resources for which you have authorization
- Protect the access and integrity of IT resources
- Abide by applicable local, state, federal laws, organizational policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted material
- Use IT resources only for their intended purpose
- Respect the privacy and personal rights of others
- Do no harm

Failure to comply with the appropriate use of these resources threatens the atmosphere for the sharing of information, the free exchange of ideas, and the secure environment for creating and maintaining information property, and subjects one to discipline. Any user of any USG organization found using IT resources for unethical and/or inappropriate practices has violated USG policy and is subject to disciplinary proceedings including suspension of system privileges, expulsion from school, termination of employment and/or legal action as may be appropriate. Although all members of the USG have an expectation of privacy, if a user is suspected of violating USG policy, his or her right to privacy may be superseded by the USG’s requirement to protect the integrity of IT resources, the rights of all users, and the property of the USG and the state. The USG thus reserves the right to examine material stored on or transmitted through its resources if there is cause to believe that the standards for appropriate use are being violated by an organization, user, or a trespasser onto its systems or networks.

The guidelines outline the responsibilities USG organizations and its users accept when using USG’s computing and IT resources. This is put forth as a minimum set of standards for all areas of the USG and may be supplemented with specific organization-level guidelines. However, such additional guidelines must be consistent with this document and cannot supersede this document. These guidelines include the use of information systems and resources, computers, telephones, Internet access, electronic mail (email), voice mail, reproduction equipment, facsimile systems, and other forms of electronic communications.
User Responsibilities

Use of USG IT resources is granted based on acceptance of the following specific responsibilities:

Use only those computing and IT resources for which you have authorization. For example, it is a violation:

- To use resources you have not been specifically authorized to use
- To use someone else’s account and password or share your account and password with someone else
- To access files, data, or processes without authorization
- To purposely look for or exploit security flaws to gain system or data access

Protect the access and integrity of computing and IT resources. For example, it is a violation:

- To use excessive bandwidth
- To release a virus or a worm that damages or harms a system or network
- To prevent others from accessing an authorized service
- To send email that may cause problems and disrupt service for other users
- To attempt to deliberately degrade performance or deny service
- To corrupt or misuse information
- To alter or destroy information without authorization

Abide by applicable laws and USG policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software. For example, it is a violation:

- To download, use or distribute copyrighted materials, including pirated software or music or videos or games
- To make more copies of licensed software than the license allows
- To operate and participate in pyramid schemes
- To upload, download, distribute, or possess pornography
- To upload, download, distribute, or possess child pornography

Use computing and IT resources only for the intended purposes. For example, it is a violation:

- To use computing or network resources for advertising or other commercial purposes
- To distribute copyrighted materials without express permission of the copyright holder
- To send forged email
- To misuse Internet Relay Chat (IRC) software to allow users to hide their identity, or to interfere with other systems or users
- To send terrorist threats or “hoax messages”
- To send chain letters
- To intercept or monitor any network communications not intended for you
- To attempt to circumvent security mechanisms
- To use privileged access for other than official duties
- To use former privileges after graduation, transfer or termination, except as stipulated by the USG organization
Respect the privacy and personal rights of others. For example, it is a violation:

- To use electronic resources for harassment or stalking other individuals
- To tap a phone line or run a network sniffer or vulnerability scanner without authorization
- To access or attempt to access other individual's password or data without explicit authorization
- To access or copy another user's electronic mail, data, programs, or other files without permission
- To disclose information about students in violation of USG Guidelines

System and Network Administrator Responsibilities

System Administrators and providers of USG computing and IT resources have the additional responsibility of ensuring the confidentiality, integrity, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately for their intended purpose and only when required to maintain the system. Any private information seen in carrying out these duties must be treated in the strictest confidence, unless it relates to a violation or the security of the system.

Cybersecurity Caveat

Be aware that although computing and IT providers throughout the USG are charged with preserving the integrity and security of resources, security sometimes can be breached through actions beyond their control. Users are therefore urged to take appropriate precautions such as:

- Safeguarding their account and password
- Taking full advantage of file security mechanisms
- Backing up critical data on a regular basis
- Promptly reporting any misuse or violations of the policy
- Using virus scanning software with current updates
- Using personal firewall protection
- Installing security patches in a timely manner

Violations

Every user of USG IT resources has an obligation to report suspected violations of the above guidelines. Reports should be directed to the institution, unit, center, office, division, department, school, or administrative area responsible for the particular system involved.
The purpose of this section is to establish the guidelines for organizing and administering cybersecurity at USG organizations.

**Cybersecurity Organization**

USG organizations must create a cybersecurity organization and program that ensures the confidentiality, integrity, and availability of all USG information assets. The program will have oversight for administration of cybersecurity standards, processes, and procedures, and will consider the effects of security 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.

Furthermore, the organization will interpret state or federal regulations and apply their requirements to USG information resources, administer programs and execute projects to meet cybersecurity objectives, and perform liaison functions between USG organizations and the USG for matters regarding cybersecurity and privacy.

Required administrative activities include, but are not limited to, the following:

1. Develop security policies, standards, processes, and procedures;
2. Determine roles and responsibilities for cybersecurity within USG organizations;
3. Develop and implement cybersecurity plans for applications, systems, and remote locations as required by local, federal, state, and USG directives;
4. Evaluate local infrastructure compliance with cybersecurity policies, processes, standards, and procedures;
5. Establish processes and procedures for access to sensitive systems and information;
6. Establish processes and procedures to minimize the likelihood of disruptions, to recover from disasters, and to respond to security incidents; and,
7. Develop programs to increase user awareness of cybersecurity issues and responsibilities.

**Information Security Officer (ISO)**

USG organizations must identify an ISO who will be responsible for establishing, maintaining, and reporting on cybersecurity roles, responsibilities, policies, standards, and procedures. This designee and the appropriate contact information must be sent annually to USG Cybersecurity, as noted in Section 5.10 of this Handbook.
Incident Management

USG organizations’ management must investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. USG organizations are required to report cybersecurity incidents.

Proper incident management includes the formulation and adoption of a written incident management plan, which provides for the timely assembly of appropriate staff that is capable of developing 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. USG organizational incident management policies and plans must be on file at USG Cybersecurity.

Cybersecurity Incident Reporting Requirements

USG organizations must establish a Cybersecurity Incident Response (CSIR) plan to respond to and manage adverse activities or actions that threaten the successful conduct of teaching, instruction, research and operations in the USG. This plan should follow existing USG policies and standards, industry best practices, and International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST) guidelines. This plan must be on file with USG Cybersecurity.

Criteria for Reporting Incidents

USG organizations’ management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. USG organizations are required to report cybersecurity incidents consistent with the security reporting requirements of this Handbook. Reports must be submitted to USG Cybersecurity per the Reporting Requirements noted in Section 5.10 of this Handbook.

Incident Follow-up Report

In addition, an incident follow-up report must be submitted that 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. Reports must be submitted to USG Cybersecurity using the ticketing system.

Incidents Involving Personal Information

USG organizations that collect, use, or maintain records containing personal information shall establish and maintain in its incident management plan, procedures for ensuring that any breach of security involving personal information, regardless of its medium (e.g., paper, electronic, verbal) immediately trigger the incident response procedures. Procedures must be documented and address, at a minimum, the following:

1. Incident Response Team. Procedures shall identify the positions responsible for responding to a breach of personal information. A response team should include, at a minimum, an escalation manager, the program manager of the program or office experiencing the breach, the ISO, the Senior Official for Privacy,
the Public Information or Communications Officer, Legal Counsel, and a representative from the USG organizations. Some incidents will require the involvement of others not mentioned above. For example, if the source of the compromised information was a computer system or database, the USG CIO should also be involved in the response activity. If the incident involves unauthorized access, misuse, or other inappropriate behavior by an employee, or the security breach involves employee’s personal information, USG organizations Personnel Officer or Human Resource Manager should be involved.

2. 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; USG organization Incident Response Team is assembled; and, the incident is addressed immediately.

3. 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 with 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;
- 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.

4. Notice to Affected Individuals. Notice to individuals when a breach of notice-triggering data elements occurs, regardless of the media involved (electronic or paper), and in accordance with criteria set forth above.

5. Breach Notification Trigger. The USG requires a notification be made to individuals when the breach involves unencrypted “Notice Triggering” personal information as defined in the section. Technically, the law is applicable to a breach involving computerized data. However, the USG has taken the position that a notification should be made when a breach of this same “Notice Triggering” data involves paper or other types of media, as the breach would expose individuals to the same financial/identity theft risk and concerns. Safeguarding all personal, confidential, or sensitive information, no matter the format, is essential to maintaining trust in USG. The objective is to make timely notification to individuals so that they may take appropriate steps to protect themselves.

**USG Computer Security Incident Management Requirements 5.3.5**

This section establishes a requirement that USG organizations establish a process for detecting and responding to security incidents.

Purpose

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

This standard establishes the requirement for USG organizations to establish an internal capability for handling computer security incidents.

Guideline

USG organizations shall establish and document an internal cybersecurity incident management capability that provides for prevention, monitoring, detection, containment, response, recovery, reporting and escalation appropriate to the level of risk and threats to the USG organization.

USG organizations’ management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. USG organizations are required to report cybersecurity incidents according to the security reporting requirements in this standard.

**USG Incident Response and Reporting Requirements 5.3.6**

This section sets minimum requirements for cybersecurity incident response and reporting.

**Purpose**

In support of the USG Computer Security Incident Management Standard, USG organizations must implement a cybersecurity incident handling capability. This standard establishes the minimum incident response and reporting requirements.

**Requirements**

1. USG organizations must implement an incident management capability including documented processes and procedures for monitoring, detection, data collection, analysis, containment, recovery, response, reporting and escalation.

2. All incident response reporting and escalation procedures must be formally documented and approved by the USG CISO.

   -Upon discovery of any incident that meets the defined criteria below:

   Cybersecurity events refer to any questionable or suspicious activity that could threaten the security of sensitive data and/or our systems infrastructure. These events may or may not have criminal implications. 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. To learn more visit http://www.usg.edu/cybersecurity/incident_management.

   -USG organizations must train employees on how to recognize and report incidents in accordance with the reporting and escalation procedures.
3. USG organizations must have a designated and recorded incident management point of contact.

4. A timely response is critical. USG organizations must report all security 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 ITS Helpdesk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3697 (Toll free within Georgia).

References

- USG Cybersecurity: [https://www.usg.edu/cybersecurity/incident_management](https://www.usg.edu/cybersecurity/incident_management)
- These documents can be found in PDF and zipped PDF formats at: [http://csrc.nist.gov/publications/nistpubs](http://csrc.nist.gov/publications/nistpubs)
  - NIST SP 800-61, Computer Security Incident Handling Guide
  - NIST SP 800-83, Guide to Malware Incident Prevention and Handling
  - NIST SP 800-28 Guidelines on Active Content and Mobile Code
  - NIST SP 800-19 Mobile Agent Security
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 organizations.

USG Information Asset Management Requirements 5.4.1

Purpose

Asset inventory is required by State asset management procedures, and is the method by which the USG maintains accountability of the 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. 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.

References

-USG IT Handbook, Section 5.8, USG Endpoint Security

USG Information Asset Protection Requirements 5.4.2

USG organizations must provide for the integrity and security of its information assets by identifying all information systems, automated files and databases for which the 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; and,

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.
Note: The definitions of Owners, Stewards, Trustees, and Users are covered in Section 9, Data Governance and Management Structure, of this Handbook.
Risk Management

Risk Management is defined as the process of identifying, controlling, and managing the impact of uncertain harmful events, commensurate with the value of the protected assets, to avoid risk or reduce it to acceptable levels. This process includes both the identification and assessment of risk through risk assessment, analysis, and the initiation and monitoring of appropriate practices in response to that analysis through a risk management program.

The USG CISO shall develop and maintain an risk management standard, processes and procedures for support of risk management across the USG and support of activities between organizations. The CISO shall maintain risk management implementation standards that the USG organizations must consider in the development of their individualized risk management plans.

USG Organizations Responsibilities

USG organizations must ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction, or disclosure and to ensure 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’ security plan, and are informed of applicable local, state, and federal policies, laws, regulations, and/or codes related to computerized information resources.

USG organizations employing information technology must establish a risk management process to identify, assess, and respond to the risks associated with its information assets. The unauthorized modification, deletion, or disclosure of information included in USG organizations files and databases can compromise the integrity of state and USG programs, violate individual right to privacy, and constitute a criminal act.

Risk Assessment and Analysis

Once the level of sensitivity of the information resources has been identified through an impact analysis, in which IT-related assets (e.g., information, people, 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. This process is referred to as a risk assessment; i.e., the probability of each threat event occurring and the resultant impact of that event on the information resources should be assessed during this process.

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.

The organization needs to decide if and when a residual level of risk may be acceptable. It is then senior management’s choice of one of the following activities pertaining to each of the identified risks to determine an appropriate risk response:

1. Mitigate the risk by implementing controls and countermeasures, or safeguards;
2. Accept the risk; 
3. Avoid the risk; or, 
4. Transfer the risk.

USG Organizations Risk Management Programs 5.5.3

The practice of risk management within a USG organization must be based upon the results of the organization’s risk analysis process. 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, 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 the USG organization will vary depending upon the nature of the organization’s information assets.

USG Risk Management Requirements 5.5.4

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.

Purpose

Risk management is an aggregation of three processes – risk assessment, risk mitigation, and controls evaluation and measurement – that help an organization ensure that processes are integrated with 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. 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.

Guidelines

USG organizations must ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction, or disclosure, and to ensure the physical security of these resources. USG organizations must ensure that users, contractors, and third parties that access the organization’s computerized information resources are informed of and abide by this standard, all
applicable organization policies, standards and procedures, and applicable federal and state laws related to computerized information resources.

USG organizations that employ information technology, must establish risk management and disaster recovery planning processes for identifying, assessing, and responding to the risks associated with its information assets.

Federal and state information technology regulations require USG information resources to undergo an Cybersecurity Risk Management process to identify the risks associated with their operation and to take steps to reduce and maintain risk at an acceptable level.

**USG Cybersecurity Risk Management Process 5.5.5**

Federal and state information technology regulations require USG information resources to undergo an 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**

Risk Management planners must communicate and collaborate with the USG organization’s Enterprise Risk Management (ERM) coordinator, at least annually.

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 endpoints and data (desktops, notebooks, servers, mobile devices, and other computer assets);
2. Inventory endpoints and data (desktops, notebooks, servers, mobile devices, and other computer assets);
3. Categorize the information system (impact/criticality/sensitivity);
4. Select and tailor baseline (minimum) security controls;
5. Supplement the security controls based on risk assessment;
6. Document security controls in system security plan;
7. Implement the security controls in the information system;
8. Assess the security controls for effectiveness;
9. Authorize information system operation based on mission risk; and,
10. Monitor security controls on a continuous basis.

**Specific Guidelines for IT/IS Risk Management**

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- ISO 27005 Information Security Risk Management (ISRM)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)
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. 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. 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.

### Security Categories

Security categories are based on the potential impact to an organization 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.

### Requirements

Data Owners shall inventory 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.

Note: The definition of Data Owners is covered in Section 9, Data Governance and Management Structure, of this Handbook.

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

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).

Note: The definitions of Information System Owner and Information Owner/Steward are covered in Section 9, Data Governance and Management Structure, of this Handbook.

The security categorization process is conducted as an organization-wide activity taking into consideration the enterprise architecture and the cybersecurity architecture. This helps to ensure that individual information systems are categorized based on the mission and business objectives of the organization. The results of the security categorization process influence the selection of appropriate security controls for the information system and also, 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.

References

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. USG organizations must classify each record 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 the 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 and regulatory actions.

3. **Confidential Information** is information maintained by a USG organization that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

Note: The Open Records Act is located at: [http://law.ga.gov/law](http://law.ga.gov/law).

In addition, **Personal Information** may occur in unrestricted/public, sensitive, and/or confidential information. Personal information is information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. 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. **Notice-triggering personal information** - specific items or personal information (name plus Social Security Number, driver’s license/Georgia identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person.

2. **Protected Health Information** - individually identifiable information created, 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. Laws require special precautions to protect from unauthorized use, access, or disclosure.

3. **Electronic Health Information** - individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers conducting electronic transactions ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure.

4. **Personal Information for Research Purposes** - personal information requested by researchers specifically for research purposes. Releases may only be made to the USG or other non-profit educational institutions in accordance with the provisions set forth in the law.

5. **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 sensitive, such as the PII on a business card, while other PII is considered Sensitive Personally Identifiable Information (Sensitive PII), as defined below.

6. **Sensitive Personally Identifiable Information (Sensitive PII)** - personally identifiable information that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, such as a Social Security number or alien number (A-number). Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if compromised.

The designated owner of a record is responsible for making the determination as to whether that record should be classified as public or confidential, and whether it contains personal and/or sensitive information. 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.

**Note**: The definition of Owner is covered in Section 9, Data Governance and Management Structure, of this Handbook.

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 participant organization to take necessary action to preserve the integrity of 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 of this Handbook, for USG organizations.
Endpoint Security

5.8

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 bi-annual USG Information Security Program Review and USG Internal Audit and Compliance.

Discovery and Inventory

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 is capable of detecting and discovering 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.

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.

Operating System (OS)/Application Patch Management

In order 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.
Implementation and Compliance 5.8.5

Endpoint security components and features must be compliant in accordance with the following dates:

<table>
<thead>
<tr>
<th>Component</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Discovery and Inventory</td>
<td>September 2015</td>
</tr>
<tr>
<td>Antivirus, Anti-malware, Anti-spyware</td>
<td>September 2015</td>
</tr>
<tr>
<td>OS/App Patch Management</td>
<td>March 2016</td>
</tr>
</tbody>
</table>

Related USG Policies, Standards and Guidelines 5.8.6

- BOR Policy Manual, Section 11
- National Institute of Standards and Technology (NIST)
- Federal Information Security Management Act (FISMA)
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 and services as well as adequate protection from known and anticipated threats. As noted in Section 5.2.2 of the IT Handbook, USG organizations are responsible for the designation of officials to fulfill key security functions and report on status of compliance with security policy, standards and procedures.

Roles and Responsibilities

5.9.1

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

Organization President or Chief Executive

The Chancellor, organization president or chief executive is responsible for ensuring that appropriate and auditable cybersecurity controls are in place to include awareness, training and education.

Information Security Officer (ISO)

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

1. Establish overall strategy for security awareness, training and education.
2. Understand program maturity and compliance.
3. Provide evidence that all users accessing information or information systems are trained in their security 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 must:

1. Understand and comply with USG organizational security policies and procedures.
2. Be appropriately trained in the acceptable use of the systems and applications to which they have access.
3. Work with management to meet training needs.
4. Be aware of actions to better protect USG organizational information and information systems. These include, but are not limited to password usage, data management, antivirus protection, incident reporting and actions to avoid social engineering attacks.
Security Awareness, Training and Education Requirements 5.9.2

USG organizations cannot protect confidentiality, integrity and availability of information and information systems 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. 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.
- Threats to cybersecurity and incident reporting.

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

Enabling Learning Objectives:

- To know where to locate within the organization the PSG’s governing information security.
- 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 information security.
- Define the location of the USG organizations’ PSG’s governing cybersecurity.
- Define the location of relevant regulatory, industry and compliance legislation and standards.
- Define confidentiality, integrity and availability (CIA).
- 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.
   - Define the USG organizations’ data management structure.
   - Define roles and responsibilities.
     - Data Owner
     - Data Trustee
     - Data Stewards
     - 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 security threats.
   - Describe how to report an incident.
     - To the USG in accordance with:
       - IT Handbook requirements.
       - Federal, state and industry legislative and/or regulatory requirements.
     - To the USG organization.

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.

References

- NIST SP 800-16 IT Security Training Requirements
- NIST SP 800-50 Building an IT Security Awareness and Training Program
The University System of Georgia (USG) has a compelling need to ensure confidentiality, integrity and availability of information technology (IT) systems and 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 security functions and report on status of compliance with security policy, standards and procedures.

**Required Reporting Activities**

1. **Cybersecurity Officer Contact Information Update**
   
   As noted in Section 5.2.2 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.

2. **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.

3. **Cybersecurity Incident Reporting Requirement**
   
   As noted in Section 5.3.6 of the USG IT Handbook, a timely response is critical. USG organizations must report all security 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 ITS Helpdesk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3697 (toll free within Georgia).

4. **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.

5. **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 the Required Reporting Diagram. USG Cybersecurity will complete the following CPR processes on an annual basis:

   - March: 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.

- April: USG Cybersecurity releases the Spring CPR survey to USG organizations. USG organizations have 30 days to complete the survey.

- May: USG Cybersecurity collects, compiles and analyzes Spring CPR survey results.

- October: USG Cybersecurity releases the Fall CPR survey to USG organizations. USG organizations have 31 days to complete the survey.

- November: USG Cybersecurity collects, compiles and analyzes Fall CPR survey results.

- December: 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.

Required Reporting Diagram:

6. 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 the Required Reporting Diagram. USG Cybersecurity will complete the following remediation/mitigation tracker processes on an annual basis:
- January: USG Cybersecurity requests USG organizations to update winter Remediation/Mitigation Trackers (trackers). USG organizations are permitted 31 days to complete the trackers.

- February: USG Cybersecurity collects, compiles and analyzes the updated winter trackers.

- July: USG Cybersecurity requests USG organizations to update summer trackers. USG organizations are permitted 31 days to complete the trackers.

- August: USG Cybersecurity collects, compiles and analyzes the updated summer trackers.

- September: 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.

**Cybersecurity Program Review**

5.10.2

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 cybersecurity professionals designated as USG organizational cybersecurity contacts. Advance succession planning in support of Continuity of Operations Planning (COOP).

2. Governance & Strategic Planning: Goal(s): Develop a cybersecurity strategy or strategies. Each strategy is supported by one or more measurable objectives.

3. Policy and Compliance: Goal(s): Develop a full life cycle policy development process, refreshment and retirement methodology based on current best practices.

4. 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.

5. Cybersecurity Incident Response: Goal(s): Track and quantify the number of USG organizations with a formal incident management capability.

6. Continuity of Operations Planning: Goal(s): Ensure the USG organizations’ COOP includes collaboration with emergency operations, planning strategies and initiatives.

7. Awareness and Training: Goal(s): Ensure each organization has a cybersecurity awareness program that is completed annually by each employee and individuals who through formal, informal, contract or other types of agreements interact with USG organizational information and information systems.

8. Data Governance & Privacy: 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.
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 Board of Regents Business Procedures Manual, 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, i.e., CIO, network director.

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, scheduled, on track, 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.

References

Federal Information Security Modernization Act (FISMA) – 2014 (Public Law 113-283)
Federal Information Processing Standards (FIPS) 199/200
NIST SP 800-30 Risk Management Guide for Information Technology Systems
NIST SP 800-53 Recommended Security Controls for Federal Information Systems
NIST SP 800-55 Performance Measurement Guide for Information Security
NIST SP 800-80 Guide for Developing Performance Metrics for Information Security
Minimum Security Standards for USG Networked Devices

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

**Software Patch Updates**  
5.11.1

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. Exceptions may be granted for patches that compromise the usability of critical applications.

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

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.

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

Host-based firewall or hosted-based intrusion prevention software for any particular type of 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.

**Passwords**  
5.11.4

USG electronic communications systems 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 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.

**Encrypted Authentication**  
5.11.5

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. In particular, 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 policy does not apply to mainframe and server tapes.

Physical Security 5.11.6

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. In light of 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.

Unnecessary Services 5.11.7

A service(s) not necessary for the intended purpose or operation of the device shall not be running.
Password Security

User Access Controls 5.12.1

USG organizations must establish policies and procedures that ensure necessary user access controls are in place for controlling the actions, functions, applications, and operations of legitimate users. The aim is to protect the confidentiality, integrity, and availability of all USG information resources.

The guiding principles in developing these standards and procedures are:

1. Users will have access to the resources needed to accomplish their duties.
2. User access applies the principles of least privilege and resource categorization as necessary tools to achieve the desired purpose.
3. User access controls will balance security and USG mission needs.

All users, whether internal, external, or temporary, and their activity on all IT systems should be uniquely identifiable. User identification should be enabled through appropriate 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. User access rights should be requested by user management, approved by system owners, and implemented by the appropriate local security administrator. User identification and access rights should be maintained in a central repository. Each USG organization should deploy cost-effective technical and procedural measures to establish user identification, implement authentication, and enforce access rights. These measures should be reviewed periodically and kept current.

USG Password Authentication Standard 5.12.2

Purpose

Passwords are an important aspect of information and information technology security. They are often the only means for authenticating users and the front line of protection for user accounts. Failure to use a strong password or using a poorly chosen password when accessing USG information assets may result in the compromise of those assets. It is the responsibility of every USG organization to implement authentication mechanisms such as passwords to access sensitive data, and the responsibility of the user to appropriately select and protect their passwords.

Scope

This security standard applies to USG organizations. This standard also applies to all users (employees, contractors, vendors, and other parties) of USG and state information technology systems or data are expected to understand and abide by the standard.

Standard

Passwords shall be the minimum acceptable mechanism for authenticating users and controlling access to USG organizations’ information systems, services and applications unless specifically designated as a public access resource.
All users (students, employees, contractors, and vendors) with access to USG information and information systems shall take the appropriate steps to select and secure their passwords.

Enforcement

Individual USG organizations are responsible for developing internal procedures to facilitate compliance with these USG security policies and standards. The standards are designed to comply with applicable laws and regulations. However, if there is a conflict, applicable laws and regulations will take precedence.

USG organizations may establish more stringent policies, standards and procedures consistent with this USG standard.

Violations of this standard could result in serious security incidents involving sensitive state, federal, sensitive or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution.

The standards will guide periodic security reviews, as well as audits by USG Internal Audit & Compliance and the state Department of Audits and Accounts (DOAA).

**USG Password Security and Composition Requirement 5.12.3**

Purpose

This section establishes a standard for protecting passwords and the frequency of change for such passwords to mitigate compromise of sensitive information.

Scope

This security standard applies to all USG organizations. This standard also applies to all USG users, including employees, contractors, vendors, and other parties.

Guidelines

1. All passwords shall be treated as sensitive, confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators and helpdesk personnel.

2. Passwords shall not be stored in clear text.

3. Users shall not write passwords down or store them anywhere in their office or publically. They shall not store passwords in a file on any computer system, including smart devices, without encryption.

4. 4a. Administrative-level passwords shall be changed every ninety (90) days.
   4b. User-level passwords shall be changed every one hundred eighty (180) days.
   4c. 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.)

5. User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.

6. Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.
7. If an account or password is suspected of being compromised, the incident must be reported to the appropriate authorities in accordance with local incident response procedures.

8. 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.

9. Access to all USG information systems and applications used to process, store, or transfer data with a security categorization of MODERATE or higher, as defined in Section 5.6.3 of this Handbook, shall require the use of strong passwords or other strong authentication mechanisms. Strong passwords shall be constructed with the following characteristics:

   - Be at least ten characters in length
   - Must contain characters from at least two of the following four types of characters:
     - English upper case (A-Z)
     - English lower case (a-z)
     - Numbers (0-9)
     - Non-alphanumeric special characters ($, !, %, ^, …)
   - Must not contain the user’s name or part of the user’s name
   - Must not contain easily accessible or guessable personal information about the user or user’s family, such as birthdays, children’s names, addresses, etc.
   - Note 1: A six-character password is acceptable if “account lockout” is enabled and set to lock or disable the account after five unsuccessful or failed login attempts. Six-character passwords must adhere to all of the characteristics noted above.
   - Note 2: Organizations may mix different characteristics regarding length and mandatory characters to obtain the same password strength. For example, a password of 11 characters containing two upper case letters, two lower case letters, two numbers, and no special characters would be permissible.

10. Password history must be enabled and configured to disallow usage of the same password for a set length of change cycles greater than four (4) times. Users and administrators must not be allowed to use the same password that has been used in the past four (4) changes. Users and administrators who have changed their user password or system password must not be allowed to change passwords immediately. This will prevent users and administrators from changing their passwords several times to get back to their old passwords.

**Enforcement**

Individual USG organizations are responsible for developing internal procedures to facilitate compliance with these USG security policies and standards. The standards are designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations will take precedence.

USG organizations may establish more stringent policies, standards and procedures consistent with this USG standard.

Violations of this standard could result in serious security incidents involving sensitive state, federal, sensitive or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution.

The standards will guide periodic security reviews, as well as audits by USG Internal Audit & Compliance and the state Department of Audits and Accounts (DOAA).
Domain Name System

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

**Domain Name System (DNS) Management 5.13.1**

**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. Footprinting and unrestricted zone transfers permit DNS zone data to be acquired by an attacker to develop an understanding of the networked resources.
2. Denial-of-service are schemes attackers use to deny availability to services.
3. Data modification and redirection occurs when attackers change zone data, permitting them to set up fake Web servers or redirect email.

**Scope**

This standard covers internal and external DNS architecture.

**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 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 located 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.

DNS Guidelines

- Domain Name System (DNS) Guidelines

References

- NIST Special Publication 800-53, Revision 4 (Security and Privacy Controls for Federal Information Systems and Organizations)
- NIST Cybersecurity Framework : PR.AC-5
- NIST Special Publication 800-81-2 (Secure Domain Name System (DNS) Deployment Guide)
- Microsoft Securing DNS (https://technet.microsoft.com/)
Identity Theft Prevention - Red Flags Rule

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.

Purpose

The USG adopts this standard and enacts this program in an effort 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, as defined in Section 5.7 of this Handbook, is any 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.

Under this standard, the program will:

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 that involves or is designated to permit multiple payments or transactions; or,

   - Any other account maintained by a USG organization for which there is a reasonably foreseeable risk of identity theft to students, faculty, staff, or other applicable constituents, or for which there is a reasonably foreseeable risk to the safety or soundness of the USG organization from identity theft, including financial, operational, compliance, reputation, or litigation risks.

2. Detect red flags that are incorporated in the program. A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

3. Respond appropriately to any red flags that are detected under this program to prevent and mitigate identity theft.

4. Ensure periodic updating of the program, including reviewing the covered accounts and the identified red flags that are part of this program.

5. Promote compliance with state and federal laws and regulations regarding identity theft protection.

The program shall, as appropriate, incorporate existing USG and institutional policies and guidelines such as anti-fraud programs and cybersecurity programs that control reasonably foreseeable risks.
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.

Alerts, Notifications, or Warnings from a Credit or Consumer Reporting Agency

Examples of these red flags 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 with respect to recently established credit relationships
   - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor

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 not consistent with the appearance of the individual presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or individual presenting the identification.
4. Other information on the identification is not consistent 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:
2. The address does not match any address in the consumer report; or,
   - The SSN has not been issued or is listed on the Social Security Administration's Death Master File.
   - 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 that 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 that of 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 not consistent 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.

Unusual Use of, or Suspicious Activity Related to, a Covered Account

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 not consistent 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 entity’s computer security system.

**Detecting Red Flags**

**Student Enrollment**

In order 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**

In order 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 identification 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.

**Consumer/Credit Report Requests**

In order 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.
Responding to Red Flags 5.14.4

Once a red flag or potential red flag is detected, the USG organization must act quickly with consideration of the risk posed by the red flag. The USG organization should quickly gather all related documentation, write a description of the situation, and present this information to the Program Administrator for determination. The Program Administrator will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic. The USG organization may take any of the following steps deemed appropriate:

1. Continue to monitor the covered account for evidence of identity theft.
2. Contact the student or applicant for whom a credit report was run.
3. Change any passwords or other security devices that permit access to covered accounts.
4. Close and reopen the account.
5. Determine not to open a new covered account.
6. Provide the student with a new student identification number.
7. Notify law enforcement.
8. Determine that no response is warranted under the particular circumstances.
9. Cancel the transaction.

Protecting Personal Information 5.14.5

In order to prevent the likelihood of identity theft occurring with respect to covered accounts, the 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 and 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 information in a secure manner. Note: Records may only be destroyed in accordance with the state’s records retention guideline.
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.
8. Use encryption devices when transmitting covered account information.
USG personnel are encouraged to use common sense judgment in securing covered account information to the proper extent. Furthermore, 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 Information & ePrivacy for advice.
Email Use and Protection

Purpose 5.15.1

USG email is provided as a tool to assist and facilitate state business, communications with students, faculty, and its representatives to conduct official business on behalf of the USG. This section establishes a standard for the appropriate use and protection of USG email systems.

Requirements 5.15.2

1. Access to email shall be governed by the USG organization’s authorization and access control and password protection policies and standards.

2. Email passwords shall be encrypted and not be stored or passed in clear text.

3. Email systems shall be protected from viruses, interception, and other malicious intentions.

4. Use of USG email systems for the creation or distribution of any disruptive or offensive messages is prohibited.

5. Mass mailings about viruses or other malware warnings shall not be distributed by general users, and shall be validated, approved, and distributed by the appropriate security administrator(s).

6. All email monitoring must be reviewed and approved by USG Cybersecurity and/or USG Legal Affairs.

7. Unauthorized email forwarding is prohibited. Email forwarding must be approved by the email account user or the USG organization’s executive management.
ePrivacy

Section Control

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
</tbody>
</table>

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

This section outlines ePrivacy requirements for USG organizations. The USG is committed to protecting the privacy of all its students, faculty, staff and other employees. Personal information will not be disclosed to third parties unless required by law.

We reserve the right to update and amend our ePrivacy standards as needed. A current version of the ePrivacy standards will be posted on the IT Handbook web site at: http://www.usg.edu/information_technology_handbook.

Definitions

The following definitions of shall, will, must, may, may not, and should are used throughout this Handbook.

1. Shall, Will, and Must indicate a legal, regulatory, standard, or policy requirement. Shall and Will are used for persons and organizations, and Must 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. The focus of should statements generally is more outcome-based; i.e., an alternate method to achieve the requirement may be developed assuming it is documented as effectively managing risk.

Implementation and Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
<th>Revision Date(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>USG Privacy Standard</td>
<td>June 2013</td>
<td>August 2013 to Cybersecurity, May 2014 to IT Handbook</td>
<td>May 2014</td>
<td></td>
</tr>
</tbody>
</table>
USG Privacy Standard

Section 6.1

Purpose 6.1.1
This section defines general privacy requirements for all USG organizations.

Standard 6.1.2
All USG participant organizations shall enact and maintain permanent privacy processes and procedures in adherence with this standard, which includes, but is not limited to, the following principles:

1. Personally identifiable information may only be obtained through lawful means.

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 required by law or regulation.

4. Personal data collected must be relevant to the purpose for which it is needed.

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.

Applicability and Compliance 6.1.3
Each USG participant organization must implement this privacy standard by:

1. Designating which position within the organization is responsible for the implementation of and adherence to this privacy standard.

2. Prominently posting the standard physically in its offices and on its intranet website, if site exists.

3. Distributing the standard to each of its employees and contractors who have access to personal data.

4. Complying with the USG Privacy Standard and all other State and Federal laws pertaining to information privacy.

5. Using appropriate means to successfully implement and adhere to this privacy policy.
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.

Information Collection and Use

6.2.1

The USG may collect some information 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 address 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.

Note: The definition of Personally Identifiable information is given in Section 5.7 of this Handbook.
Facilities

Section Control

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
</tbody>
</table>

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
</table>
**Introduction**

Protection for IT equipment and personnel requires well-designed and well-managed physical facilities. The process of managing this physical environment includes defining the physical 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 business interruptions from damage to IT equipment and personnel.
# Bring Your Own Device (BYOD) Standard

## Section Control

### Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
</tbody>
</table>

## Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Introduction

This section establishes the standards and procedures for end users who are connecting a personally-owned device to a University System of Georgia (USG) network for business purposes.

Definitions

The following definitions of At Rest, Bring Your Own Device (BYOD), Compliance Date, Confidential Data, In Transit, Public Data, Prior Approval, Sensitive Data, Stored and Transition Period are used throughout this section.

1. **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.

2. **Bring Your Own Device (BYOD)**: Refers to employees taking their own personal device to work in order to interface to the participant organization’s network resources.

3. **Compliance Date**: The date by which the participant organization is expected to comply with the policy or standard.

4. **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.

5. **In Transit**: Data on the move from origin to destination.

6. **Public Data**: Data elements that have no access restrictions and are available to the general public. Also can be designated as unrestricted data.

7. **Prior Approval**: A process by which all users must gain approval prior to working with, utilizing, or implementing a process or procedure.

8. **Sensitive Data**: 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 participant 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.

9. **Stored**: Data held or at rest, either locally or in the cloud.

10. **Transition Period**: A period of time whereby an object moves from one state or level to another.

Implementation and Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
<th>Revision Date(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Purpose</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td></td>
</tr>
<tr>
<td>8.2</td>
<td>Applicability</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td>January 2014</td>
</tr>
<tr>
<td>8.3</td>
<td>Standards</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td></td>
</tr>
<tr>
<td>8.4</td>
<td>Standard Non-Compliance</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td></td>
</tr>
<tr>
<td>Section Number</td>
<td>Section Name</td>
<td>Compilation Date</td>
<td>Published Date</td>
<td>Compliance Date</td>
<td>Revision Date(s)</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>8.5</td>
<td>Appendix A: Employee Declaration</td>
<td>October 2013</td>
<td>October 2013</td>
<td>October 2014</td>
<td></td>
</tr>
</tbody>
</table>
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.
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, back up 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 IT Handbook for up-to-date standards and guidance.
Standards

Section 8.3

Prior Approval 8.3.1

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 vice chancellor and chief information officer (VC/CIO). Participant organizations will establish and document local policies consistent with this prior approval standard.

2. Participant organizations will establish consistent, documented, and repeatable processes that are consistent with this prior approval standard and can be considered auditable.

Security 8.3.2

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 Chief Information Security Officer (CISO), the information security officers (ISOs) of the participant organizations, and/or other delegated designees. Participant 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 in order to identify unusual usage patterns or other suspicious activity. This monitoring is necessary in order 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 participant organization resources as it relates to personally-owned devices.

8. Managers will immediately report such incidents to the USG CISO or the participant organization ISO as appropriate.
USG Intellectual Property 8.3.3

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.

Device and Application Support 8.3.4

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.”
Standard Non-Compliance

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

I, __________________________, have read and understand the USG BYOD Standard and any augmenting participant organizational 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
Data Governance and Management Structure

Section Control

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
</tbody>
</table>

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
</table>
Introduction

Information, in all forms, is a strategic asset to the University System of Georgia (USG), including each USG institution. The purpose of this section is to provide guidelines for the management and access to data, which is critical to the administration of USG participant organizations.

Definitions

The following definitions of shall, will, must, may, may not, and should are used throughout this Handbook.

Shall, Will, and Must: indicate a legal, regulatory, or policy requirement. Shall and Will are used for persons and organizations, and Must for inanimate objects.

May: indicates an option.

May Not: indicates a prohibition.

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. The focus of “should” statements generally is more outcome-based; i.e., an alternate method to achieve the requirement may be developed assuming it is documented as effectively managing risk.

Implementation and Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
<th>Revision Date(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>May 2014 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>May 2014 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>May 2014 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>May 2014 to IT Handbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section Number</td>
<td>Section Name</td>
<td>Compilation Date</td>
<td>Published Date</td>
<td>Compliance Date</td>
<td>Revision Date(s)</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------</td>
<td>------------------</td>
<td>----------------------------------------------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
Section 9.1

Purpose

While USG participant organization information may reside in paper format, in different database management systems, or on different machines, these data, in the aggregate, may be thought of as forming a single, logical database. These data will be called institutional data. This section will describe the roles and responsibilities of stewardship for, and procedures for establishing access to, institutional data.

It is the desire of the USG that all institutional data be used with appropriate and relevant levels of access and with sufficient assurance of its security and integrity in compliance with existing laws, rules, and regulations. The goal of this section is to provide reasonable guidance to USG participant organizations to increase the value and security of data by use of appropriate guidelines, procedures and methods.

Material in this section has been taken from the following sources:

1. Georgia State University, Data Stewardship and Access Policy for University Information
2. University of Maryland, Baltimore County. UMBC Data Management Structure 6/18/2003, draft version

Scope and Restrictions

This section applies to institutional data only, as defined below, and is intended to improve access to these data by employees for conducting organization business. In all cases, applicable statutes, laws, rules, and regulations that guarantee either protection or accessibility of organizational records will take precedence over this section. While this section is especially pertinent to information stored electronically, it is applicable to all information, such as paper, microform, and video, as well as the content of confidential meetings and conversations.

This section does not apply to notes and records that are the personal property of individuals in the participant organization community and is not directed to data whose primary purpose is scholarly; e.g., instructional material, research notes, etc.

The scope of this section is to have broad application, particularly with respect to data and information resources, which have impact on organizational operation. Data that may be managed locally may also have significant impact if it is used in a manner that can impact organization operations. It is expected that the intent of this section be extended in analogous manner to all data and information used at all operational levels of the participant organization.

Institutional Data Definition

A data element is considered institutional data if it provides support to, and meets the needs of, units of the institution. Examples of institutional data include, but are not limited to, many of the elements supporting financial management, student curricula, payroll, personnel management, and capital equipment inventory.

Information may be considered institutional data if it satisfies one or more of the following criteria:
1. Data used for planning, managing, reporting, or auditing a major administrative function;

2. Data referenced or used by a participant organization to conduct organization business;

3. Data included in an official participant organization administrative report; or,

4. Data used to derive an element that meets any of the criteria above.

**System Data Definition**

A data element is considered system data if it is created by the USO and used by the USO for official purposes. Examples of system data include, but are not limited to, institutional enrollment information, financial information, and data warehouse information.

Information may be considered system data if it satisfies one or more of the following criteria:

1. Data included in the USG Data Warehouse;

2. Data that serve the policy development of the Board of Regents (BOR);

3. Data that inform decisions for, or operating, planning, managing, or auditing a major administrative function of, the USG; and,

4. Data used to produce USG reports for internal and external constituencies.
Data Management Structure

A data governance and management structure is required at each USG institution, the USO, the GPLS, and the Georgia Archives. The data management structure will demonstrate accountabilities for the data assets of the entity to ensure proper use and handling of data being read, created, collected, reported, updated or deleted.

The data management structure should identify the offices/positions (including identifying incumbent) responsible for fulfilling the roles defined herein.

**Data Governance and Management Committee (USO and USG Participant Organizations) 9.2.1**

A Data Governance and Management Committee is responsible for defining and managing implementation of the policies and procedures for the data governance and management functions at the USO and at each USG participant organization.

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

1. Defining data management roles and responsibilities herein and in other policy and procedure documentation;

2. Collating and maintaining documentation pertaining to data governance and management policy and procedure in a centralized and easy-to-access location for the participant organization staff;

3. Identifying the Data Governance and Management Committee structure and membership; and,

4. Assisting the chairs of the functional committees to ensure effectiveness.

**Data Owner 9.2.2**

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

The USO is responsible for all data being read, created, collected, reported, updated or deleted by offices of the USO collective. As the chief executive officer, the USG Chancellor is identified as the data owner of the USO data.

Data owners have the responsibility for the identification, appointment and accountability of Data trustees.

Data owners will inform the participant organization’s Data Governance and Data Management Committee of their data trustee appointments including office, name, and contact information of the incumbent.

**Data Trustees 9.2.3**

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

Responsibilities of the data trustees include, but are not necessarily limited to:

1. Ensuring that data accessed and used by units reporting to them is done so in ways consistent with the mission of the office and participant organization;

2. The identification, appointment and accountability of data stewards within the functional area(s) for which they are responsible. The data trustees will inform the participant organization's Data Governance and Data Management Committee of their data trustees appointments, including office, name, and contact information of the incumbent;

3. Participating as a member of the strategic data governance and management committee; and,

4. Communicating concerns about data quality to the data owner.

The participant organization’s chief information officer (CIO) and the information security officer (ISO), as defined in Sections 1.1 and 5.2.2 of this Handbook, respectively, whether or not designated as data trustees, have the responsibility for ensuring that a technical infrastructure is in place to support the data needs and assets, including availability, delivery, access, and security across the entirety of their operational scope.

The data trustees of the USG participant organizations are normally the counterpart of the other.

Data Stewards

Data stewards, designated by the data trustees, are offices/positions responsible for the data being read, used, created, collected, reported, updated or deleted, and the technology used to do so, in their functional areas. Positions held by the data stewards normally would report directly to the data trustee. Data stewards recommend policies to the data trustees, and establish procedures and guidelines concerning the access to, completeness, accuracy, privacy, and integrity of the data for which they are responsible. Individually, data stewards act as advisors to the data trustees and have management responsibilities for data administration issues in their functional areas. Depending on the size and complexity of a functional unit, it may be necessary, and beneficial, for a designated data steward to identify associate data stewards to manage and implement the stewardship process.

Responsibilities of the data stewards include, but are not necessarily limited to:

1. Ensuring data quality and data definition standards are met.

2. Identifying the privacy level as unrestricted, sensitive, or confidential, for functional data within their area(s) of supervision/direction.

3. Establishing authorization procedures with the USG participant organization's Data Governance and Data Management Committee and/or CIO to facilitate appropriate data access as defined by institutional/office data policy and ensuring security for that data.

4. Developing standard definitions for data elements created and/or used within the functional unit. The data definition will extend to include metadata definitions as well as the root data element definition.
5. Working with the USG participant organization’s Data Governance and Data Management Committee, identifying and resolving issues related to stewardship of data elements, when used individually or collectively, that cross multiple units or divisions. For example, the individual data element “Social Security Number” may have more than one data steward since it is collected or used in multiple systems, such as financial, human resources, and student systems. Resolving stewardship issues for “Full-time Student” would be an example of using multiple data elements collectively to garner the informational item.

6. Participating as a member of the functional data governance and management committee(s) as appointed by the data trustee.

7. Communicating concerns about data quality to the data trustees.

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

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

1. Data Definer is responsible for:
   - Defining data in the best interest of the organization;
   - Making the definition of data available to the organization; and,
   - Communicating concerns about data quality to the data steward or data trustees.

2. Data Creator is responsible for:
   - The accuracy of data being captured, created or entered;
   - The timeliness of data being captured, created or entered;
   - Defining the processes by which the technologies capture, create, or enter the data to be used; and,
   - Communicating concerns about data quality to the data steward or data trustees

3. Data Reader is responsible for:
   - The integrity/security of data being read/used; and,
   - Communicating concerns about data quality to the data steward or data trustees.
By default, all institutional data will be designated as internal data for use within a participant organization or to satisfy external reporting requirements to the USG BOR, and to state, federal, or other external agencies. Employees will have access to these data for use in the conduct of participant organization business. These data, while available within the participant organization, are not designated as open to the general public unless otherwise required by law. The permission to view or query institutional data should be granted to all data users for all legitimate participant organization purposes.

As part of the data definition process, data stewards will assign each data element and each data view in institutional data to one of three categories: unrestricted, sensitive, and confidential.

Note: In some circumstances, as long as specific identifying data elements are removed, a data view may include elements of institutional data that would otherwise be sensitive or confidential.

**Unrestricted Data**

Where appropriate, data stewards may identify institutional data elements that have no access restrictions as available to the general public. These data will be designated as unrestricted or public data.

**Sensitive Data**

Where necessary, data stewards may specify institutional data elements as sensitive 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 participant organization.

The specification of data as sensitive should include reference to the legal or externally imposed constraint that requires this restriction, the categories of users typically given access to the data, and under what conditions or limitations access is typically given.

**Confidential Data**

Where required, data stewards may identify institutional data elements as confidential, for which the highest levels of restriction should apply due to the risk or harm that may result from disclosure or inappropriate use.

This includes information whose improper use or disclosure could adversely affect the ability of the participant organization 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.
Data Access will work together to define a single set of procedures for requesting access to sensitive elements of institutional data, and to document these data access request procedures.

**Data Access**

Data stewards at the participant organization are responsible for developing and obtaining approval of data access procedures and approving all requests for data access via these procedures. It is recommended that such a process be developed that includes the following steps:

1. Requests for access must be made in writing to the appropriate functional data steward. Such requests must include approval by the requestor’s supervisor or management, and should be specific as to the data needed and the purpose for accessing the data. All requests are maintained for use in case of a need to audit access permissions.

2. Upon approval by the functional data steward, the request is forwarded to the data administration unit of the participant organization’s Information Technology (IT) department for technical implementation via provisioning of accounts, login ids, or view access.

3. The requestor will be notified of their access, and will be provided a copy of the participant organization’s Data Stewardship & Access Policy, the relevant functional guidelines for use, and any restrictions on the data, such as the Family Educational Rights and Privacy Act regulations.

4. All data access will be reviewed and renewed on an annual basis by each functional data steward to ensure that the access remains appropriate.

Note: Permission to access data does not necessarily imply permission to change data. Data stewards will ensure that the proper access rights, such as read, write, modify, or delete, are given to users who request data access.

**Data Documentation**

Data stewards are responsible for documenting the data maintained within their functional area. This documentation should include, at a minimum:

1. Data name;
2. Data description;
3. Data sensitivity;
4. Data location;
5. Data retention; and,
6. Data backup plan.

Data stewards also have responsibility for documenting the meta-data about their data so that users are aware of the definitions, restrictions, or interpretations, and other issues that ensure the correct use of the data.
USG participant organizations should focus on two critical areas as they consider protection of institutional data: privacy and security. Privacy deals with the classification and release of protected data, while Security deals with the protection or confidentiality, integrity, and availability of data.

The protection of institutional data is governed by a growing collection of federal and state laws relating to privacy and security. All USG participant organizations are morally, and now legally, responsible for the protection and integrity of the data they create and maintain at their organizations. Through a number of legal statutes and regulations, participant organizations now have a legal responsibility for protection of student, employee, and faculty information.

A participant organization is responsible for complying with all current laws and regulations concerning data privacy and security. The participant organization should identify an individual or group that will have responsibility for compliance with new regulations.

The following sections describe the major current laws that effect educational institutions and organizations. Due to the rapid changes in information technology and privacy requirements, however, new laws are being introduced at a rapid pace. Each USG participant organization must be vigilant and stay aware of new legal requirements in the Privacy and Security areas.


**Family Education Rights and Privacy Act (FERPA)**  

The primary law that governs the privacy of educational information is the Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g(b).

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing “personally identifiable education information,” such as grades or financial aid information, without the student’s written permission. FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers.

Generally, institutions must have written permission from the student in order to release any information from a student’s education record. However, FERPA does allow institutions to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

1. School officials with legitimate educational interest;
2. Other schools to which a student is transferring;
3. Specified officials for audit or evaluation purposes;
4. Appropriate parties in connection with financial aid to a student;
5. Organizations conducting certain studies for or on behalf of the school;
6. Accrediting organizations;
7. To comply with a judicial order or lawfully issued subpoena;

8. Appropriate officials in cases of health and safety emergencies; or,
9. State and local authorities, within a juvenile justice system, pursuant to specific State law.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA) 9.5.2**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to protect the rights of patients and participants in certain health plans. In 2000, the federal Department of Health and Human Services adopted copious regulations granting consumers the right to receive written notice of the information practices of entities subject to HIPAA.

Colleges and universities that are affiliated with health care providers are considered covered entities, and participant organizations must provide written notice of their affiliated health care provider’s electronic information practices. Most employer-sponsored health plans also are considered to be “entities” subject to HIPAA. As a result, various compliance obligations are imposed on colleges and universities that sponsor and administer such plans.

HIPAA generally requires covered entities to:

1. Adopt written privacy procedures that describe, among other things, who has access to protected information, how such information will be used, and when the information may be disclosed;
2. Require their business associates to protect the privacy of health information;
3. Train their employees in their privacy policies and procedures;
4. Take steps to protect against unauthorized disclosure of personal health records; and,
5. Designate an individual to be responsible for ensuring the procedures are followed.

**Electronic Communications Privacy Act (ECPA) 9.5.3**

The Electronic Communications Privacy Act (ECPA) broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. Protection of the “contents” of such communications, however, extends only to information concerning the “substance, purport, or meaning” of the communications.

In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved. As a result, the monitoring by institutions of students’ network use or of network usage patterns, generally, would not be prohibited by the ECPA, as long as the substance of the communication was not made public.

The ECPA will come into play when an institution is forced to monitor or intercept student, faculty, or employee electronic communications such as e-mail. The effect of the law may depend on the type of person being monitored and the person’s association with the institution, as a student, faculty member, or employee, and whether the communication system is considered a public or private system.

The ECPA also contains specific exceptions allowing disclosures to law enforcement agencies under certain circumstances.

**USA Patriot Act 9.5.4**

The USA Patriot Act can effect educational institutions in many ways. Probably the most significant effect is that it potentially prohibits institutions from revealing the very existence of a law enforcement investigation. All
institutions should ensure that they have worked with their legal staff to produce written procedures on how to deal with law enforcement information requests. Any institution employee faced with a request from law enforcement should follow these procedures.

**TEACH Act**

The TEACH Act relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use technology materials in educational settings. Institutions that want to take advantage of the relaxed copyright restrictions must limit “to the extent technologically feasible” the transmission of such content to students who actually are enrolled in a particular course, and they must use appropriate technological means to prohibit the unauthorized retransmission of such information.

In other words, the TEACH Act may require institutions to implement technical copy protection measures and to authenticate the identity of users of electronic course content.

**Gramm - Leach - Bliley Act (GLBA)**

The Gramm – Leach – Bliley Act (GLBA), enacted in 1999, was largely directed at financial institutions and creates obligations to protect customer financial information. However, it has been determined that colleges and universities are also covered by the act.

The GLBA has two major sections: privacy and security. The Federal Trade Commission's (FTC) regulations implementing the GLBA specifically provide that colleges and universities will be deemed to be in compliance with the privacy provisions of the GLBA if they are in compliance with FERPA. Therefore, GLBA privacy requirements should not affect educational institutions. They should therefore focus mainly on the security sections of the GLBA.

The cybersecurity, or Safeguard, section has five major requirements that a USG participant organization must follow:

1. Designate one or more employees to coordinate the security safeguards;
2. Identify and assess the risks to customer information in each relevant area and evaluate the effectiveness of the current safeguards;
3. Design and implement a safeguards program and regularly monitor and test it;
4. Select appropriate service providers and contract with them to implement safeguards; and,
5. Evaluate and adjust the program in light of relevant circumstances or the results of testing.

**Computer Fraud and Abuse Act (CFAA)**

The Computer Fraud and Abuse Act (CFAA) criminalizes unauthorized access to a “protected computer” with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer. A “protected computer” is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States. A participant organization may use this law when there has been a break-in of their computer systems.
Learning Management System (LMS)

Section Control

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016</td>
<td>PDF, structure and format</td>
<td>Initial redesign referenced in a new structure and format.</td>
</tr>
</tbody>
</table>

Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

This section establishes the standards and procedures for end users of the University System of Georgia (USG) Learning Management System (LMS).

Definitions

The following definitions of shall, will, must, may, may not, and should are used throughout this Handbook.

- **Shall**, **Will**, and **Must** indicate a legal, regulatory, standard, or policy requirement. **Shall** and **Will** are used for persons and organizations, and **Must** for inanimate objects.

- **May** indicates an option.

- **May Not** indicates a prohibition.

- **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. The focus of should statements generally is more outcome-based; i.e., an alternate method to achieve the requirement may be developed assuming it is documented as effectively managing risk.

Implementation and Compliance

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Section Name</th>
<th>Compilation Date</th>
<th>Published Date</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Applicability</td>
<td>June 2013</td>
<td>March 2015</td>
<td>March 2016</td>
</tr>
<tr>
<td>10.2</td>
<td>Service Description</td>
<td>January 2014</td>
<td>March 2015</td>
<td>March 2016</td>
</tr>
<tr>
<td>10.3</td>
<td>Participation Model</td>
<td>June 2013</td>
<td>March 2015</td>
<td>March 2016</td>
</tr>
<tr>
<td>10.4</td>
<td>Governance</td>
<td>June 2013</td>
<td>March 2015</td>
<td>March 2016</td>
</tr>
<tr>
<td>10.5</td>
<td>Resource Model</td>
<td>June 2013</td>
<td>March 2015</td>
<td>March 2016</td>
</tr>
</tbody>
</table>
Applicability

Introduction

This standard applies to all USG units.

This standard is complementary to any previously implemented policies and standards covering acceptable use of and access to any element of the enterprise network. Always consult the USG IT Handbook for up-to-date standards and guidance.
Service Description

Services provided as part of the GeorgiaVIEW LMS are detailed in the Service Level Agreement (SLA). The SLA covers:

1. Agreement Overview

2. Goals & Objectives

3. Stakeholders

4. GeorgiaVIEW Community

5. Learning Management System Environment
   - GeorgiaVIEW Desire2Learn License
   - GeorgiaVIEW D2L Production Environment
   - GeorgiaVIEW D2L Test Environment
   - GeorgiaVIEW D2L Functional Development Environment
   - GeorgiaVIEW Dependent Infrastructure Hardware and Services
   - Disaster Recovery
   - GeorgiaVIEW Desire2Learn Application System Component Failure Contingencies

6. Learning Management System Integrations
   - Student Information System Batch Integration
   - D2L External Authentication (if selected)
   - 3rd Party Integrations (existing through implementation)

7. Learning Management System Performance and Escalations

8. Security

9. Learning Management System Support
   - Customer Support
   - Service Request
   - Note
   - ITS Customer Support/Service Request Process
   - User Support
   - User Support Process

10. Learning Management System Service Availability

A copy of the document can be accessed directly [here](#).
The system standard for the LMS is Desire2Learn (D2L). 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 vice chancellor and chief information officer (VC/CIO), vice chancellor for academic affairs (VC/AA), and the executive vice chancellor and chief academic officer (EVC/CAO) to the Chancellor.

As noted in the Task Force recommendation, 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. The downsides from allowing multiple LMS platforms on a single campus strongly outweigh the potential benefits of this kind of flexibility at an institution.
Governance

Section 10.4

**Business Owner**

The business owner of the learning management system is USG Academic Affairs. The business owner will make all functional decisions regarding the LMS and appoint an LMS Executive Committee.

**LMS Executive Committee**

The LMS Executive Committee will provide strategic oversight of the USG learning management system. This committee will:

1. Provide a prioritized recommendation for the addition or reduction of LMS functionality to the USG VC/CIO, VC/AA, and the vice chancellor and chief financial officer (VC/CFO) no later than 1 December of each year.

2. Review system availability and customer satisfaction of the LMS system annually and provide recommendations to the VC/CIO and the VC/AA.

3. Perform such tasks as assigned by USG Academic Affairs.
Resource Model

Section 10.5

General Description

The USG Enterprise LMS program (GeorgiaVIEW) lowers institutional costs 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.
2. The revenue chargeback is based on the institutional FTE.
3. The revenue chargeback is the sum of what institutions were being charged for the previous LMS (Blackboard Vista 8) plus the funding increase the institutions received in the LMS budget line starting in FY2013. This ensures that the LMS chargeback is cost-neutral to institutions.
4. To preserve the economies of scale, all institutions are required to participate in this effort, and should use D2L as their LMS exclusively. However, as noted in Section 9.3, 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.

Licensing and Hosting Costs

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. This waiver will be reviewed periodically by USG Academic Affairs to consider the utility of continuing the waiver.

Georgia Regents University and Georgia Southern University were granted temporary waivers to provision additional LMS hosting services. These waivers will be reviewed periodically by the VC/CIO to consider the utility of continuing the waiver.

Annual Escalator

The contract annual escalator is CPI-based. This escalator, from 2012 until 2016, is included in the state funds allocated to the institution. As such, there are no annual escalators in the D2L Software as a Service (SaaS) service.
**TrueUps**

**License TrueUps**

The D2L license cost is FTE-based. While there are allowances in the contract for modest FTE growth, FTE growth beyond contract limits will result in increased charges that are allocated on an annual basis as part of the normal fiscal model. The increased charges, should they ever occur, will be institution FTE-based.

**Hosting TrueUps**

The D2L hosting model is consumption-based using storage as the demonstrative metric. While there are allowances in the equipment planning to cover the hosting costs for five (5) years, storage growth beyond these planning limits will result in increased charges that are allocated on an annual basis as part of the normal fiscal model. The increased charges will be institution storage consumption-based.

**Equipment Refresh**

Equipment refresh is based on a five (5) year cycle. A small portion of the institution charges is saved in a LMS reserve account annually so that equipment may be purchased as needed.

**Change Management**

**Major Upgrades**

Major upgrades to the LMS will occur annually during the December holiday break.

**System Upgrade Initiatives**

Additional functionality identified by the LMS Executive Committee and approved for funding by the Chancellor will be implemented normally during the December holiday break.

**Institution Upgrade Initiatives**

By acting as a consortium, institutions can realize additional savings by purchasing additional functionality in the LMS.