University of Guam Office of Information Technology

University Policy Manual (IT-UPM)

Last updated: August 11, 2018

Table of Contents

1.00 | University of Guam Policy / Procedure Face Sheet

Policy Type	[ ] Board; [ ] Board-approved; [ ] President; **[X] President-approved**; [ ] Other _____				
Policy/Procedure Manual Name	**UOG Office of Information Technology Procedures, Regulations, and Policies Manual (IT-UPM)**				
Article No.	II	**Article Title**	Policies of the UOG Board of Regents		
Insert Policy / Procedure in		**UOG Office of Information Technology Procedures, Regulations, and Policies Manual**			
Approval Authority	President	**Effective**	08/13/2018	**Most Recent Review**	08/13/2018
Responsible Executive	Chief Information Officer	**Resolution No** (or other tracking no).	08-07	**Date of Next Required Review** (date set by Board)	04/23/2021
Responsible Office	Office of Information Technology	**Revision Tracking**	08/13/2018		
Policy/Procedure Contact & Website where document is maintained	671.735.2630; helpdesk@triton.uog.edu; https://www.uog.edu/policy-procedures-library/				
Who Should Review (not in specific order)	[X] Chief Information Officer; [X] Office of Information Technology Administrator(s); [X] UOG IT Advisory Committee; [ ] Human Resources Office; [ ] Business Office; [ ] Facilities & Maintenance; [ ] Institutional Safety Committee; [ ] Faculty Senate; [ ] Faculty Union; [ ] Student Government Association; [X] Administrative Council; [X] Academic Officers Council; [ ] Vice President Administration & Finance; [ ] Senior Vice President for Academic & Student Affairs; [ ] UOG Legal Counsel; [X] UOG President; [ ] UOG Board of Regents; [ ] Guam Legislature; [ ] Governor of Guam				
Initiation / Review / Consultation / Approval History	Original content from 2000 RRPM and UOG Board of Regents Resolution 08-07 (2/21/2008); Content extracted and made into IT-PRP Manual; Guidelines and standards original documents for Office of Information Technology, approved by President Thomas W. Krise 08/13/2018.				
NOTE: All approved changes to policy/procedures need to be made on the hardcopy of this document within 5 workdays and posted on https://www.uog.edu/policy-procedures-library/ within 10 workdays from the date approved.					

1.00.1 FEEDBACK

1.00.1.1 University faculty, staff, students, administrators, or other authorized users may provide feedback about this policy / procedure face sheet through our contact information below:

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630
HelpDesk: (671) 735-2630
Fax: (671) 734-9422
Email: helpdesk@triton.uog.edu
Website: https://it.uog.edu

1.01 | Introduction

Effective Date: 8/13/2018 | **Revised Date**: 08/13/2018

1.01.1 INTRODUCTION

The University of Guam (UOG) is the primary U.S. Land Grant institution accredited by the Western Association of Schools and Colleges (WASC) Senior College and University Commission (WSCUC) serving the post-secondary needs of the people of Guam and the region.

Within its capacity, the University's Office of Information Technology (OIT) provides faculty, staff, students, administrators and other authorized users with access to appropriate information technology (IT) resources that are integral and critical to the University's mission.

The IT University Policy Manual (IT-UPM) provides guidance with regards to IT operations at UOG. This living manual will provide, and be continuously updated with, current university policies, procedures, regulations, standards, best practices, and guidelines under which the acquisition, development, planning, design, construction / renovation, management and operation of UOG information technology facilities and systems shall be accomplished. In addition, this manual defines the organizational scope of Information Technology at the University of Guam.

1.01.2 OUR VISION

The Office of Information Technology strives to be a regionally strategic and innovative IT organization that provides a **leading edge technology** environment for students, faculty and staff to advance the University mission and goals.

1.01.3 OUR MISSION

We advance the vision and goals of our university by contributing to educational innovation and providing agile, cost-effective, and reliable technology services and facilities to our campus community. As a reflection of these values, our organizational slogan is:
Educate. Innovate. Connect.

1.01.4 OUR VALUES

At the Office of Information Technology, we are:

- Collaborative and Service-Oriented
- Accountable and Transparent
- Innovative and Secure
- Agile and Efficient

1.01.5 CONTACT INFORMATION

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630 | HelpDesk: (671) 735-2630
Fax: (671) 734-9422 | Email: helpdesk@triton.uog.edu | Website: https://it.uog.edu

1.05 | Scope and Management of IT University Policy Manual (IT-UPM)

Effective Date: 8/13/2018 | **Revised Date**: 08/13/2018

1.05.1 SCOPE OF IT-UPM

This UOG IT Policies and Procedures Manual (IT-UPM) serves several purposes.

- Primarily, it sets forth the essential standard components UOG organizations must follow to meet statutory or regulatory requirements of the federal government and the Government of Guam, Board of Regents (BOR) policy mandates, and Information Technology best practices.
- Secondly, it is designed to provide new faculty, staff, students, administrators and other authorized IT users within the UOG the necessary information and tools to perform effectively.
- Finally, it serves as a useful reference document for seasoned professionals at UOG organizations who need to remain current with changes in federal and Guam 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-UPM, while focusing on UOG standards, also offers ready access to important policies, statutes and regulations that will aid UOG IT users in his or her daily performance of duties.

Finally, this IT-UPM, its policies, regulations, procedures, standards, best practices, and guidelines supersede the UOG IT Policy document published in February 21, 2008, as established by BOR Resolution No. 08-07.

1.05.2 WHO SHOULD READ THE IT-UPM

All members of the university community should read this manual.

1.05.3 MANAGEMENT OF UNIVERSITY POLICY MANUAL

The Chief Information Officer, working with the various IT Governance groups defined in this manual, maintains this manual and is responsible for making sure it is updated and posted on the UOG Policies and Procedures website.

1.05.3.1 The UOG IT UNIVERSITY POLICY MANUAL (IT-UPM) shall be updated as necessary to reflect changes in the UOG's academic, administrative, or technical environments, or applicable laws and regulations. The UOG Chief Information Officer (CIO) shall be responsible for overseeing a periodic review of this manual and communicating any changes or additions to appropriate UOG stakeholders.

1.05.3.2 The IT-UPM may be augmented, but neither supplanted nor diminished, by additional policies and standards adopted by UOG.

1.05.3.3 The campus, through consultation with campus officials and key stakeholders, must develop policies, standards, and implementation procedures referenced in the UOG IT UNIVERSITY POLICY MANUAL (IT-UPM).

1.10 | Office of Information Technology Organization

Effective Date: 08/13/2018 | **Revised Date**: None

1.10.1 ABOUT THE OFFICE OF INFORMATION TECHNOLOGY

The Office of Information Technology strives to be a regionally strategic and innovative IT organization that provides a leading-edge technology environment for students, faculty and staff to advance the University mission and goals.

Information Technology plays a significant role at the University of Guam. Our organization understands the challenges that face our students, faculty, and staff and we continuously strive to produce a higher quality of services designed to meet the expectations of the campus community.

The Office of Information Technology empowers students, faculty and staff with technology-based solutions that promote curricular and co-curricular success. We utilize technologies to enable process automations and efficiencies where possible.

Finally, we advance the vision and goals of our university by contributing to educational innovation and providing agile, cost-effective, and reliable technology services and facilities to our campus community. As a reflection of these values, our organizational slogan is:
Educate. Innovate. Connect.

1.10.2 INFORMATION TECHNOLOGY ORGANIZATIONAL STRUCTURE

The current organizational structure of the Office of Information Technology is depicted in the following organizational chart diagrams included below (Figure 1 and Figure 2).

As a crucial organization vital to the enterprise operations of the University of Guam, the Office of Information Technology will continuously strive to redefine and reorganize its structure to meet the University's needs.

Figure 1

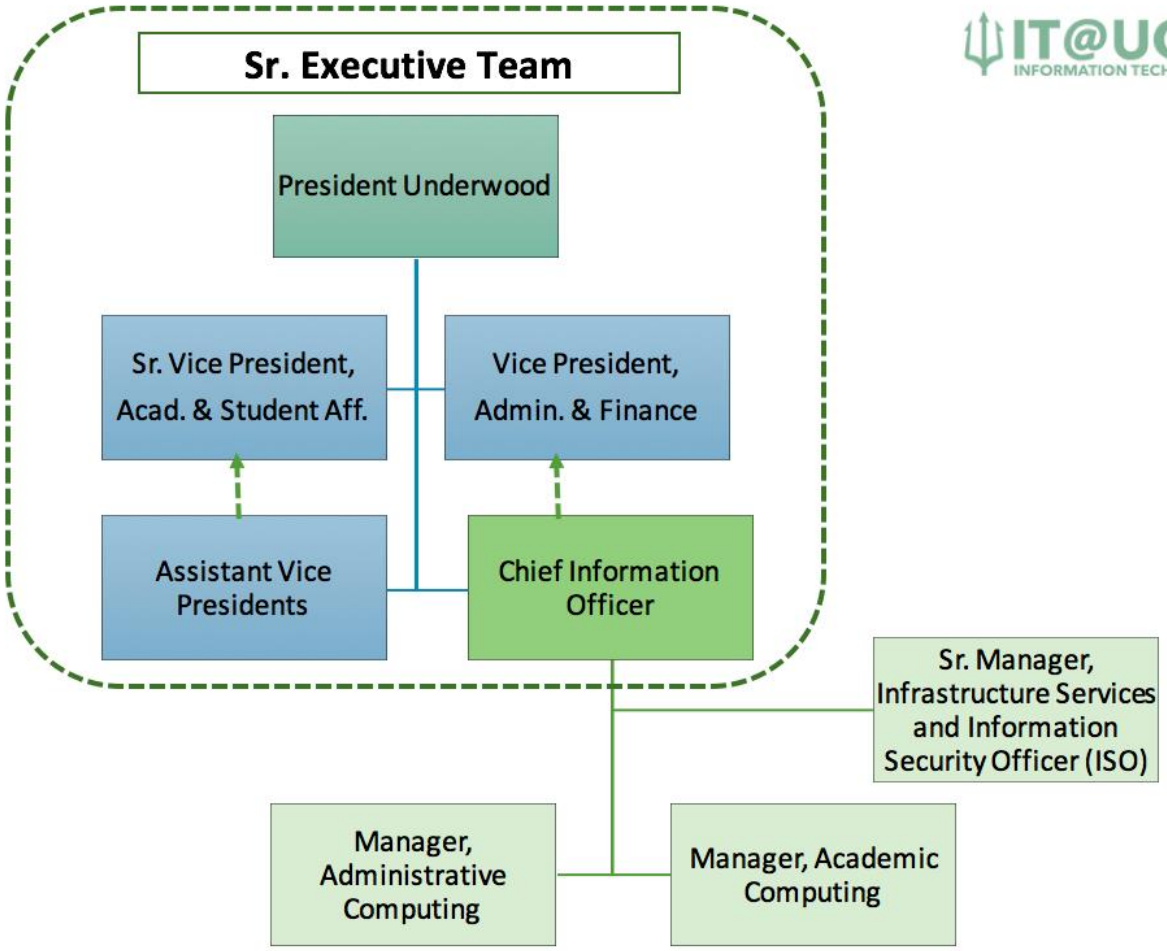
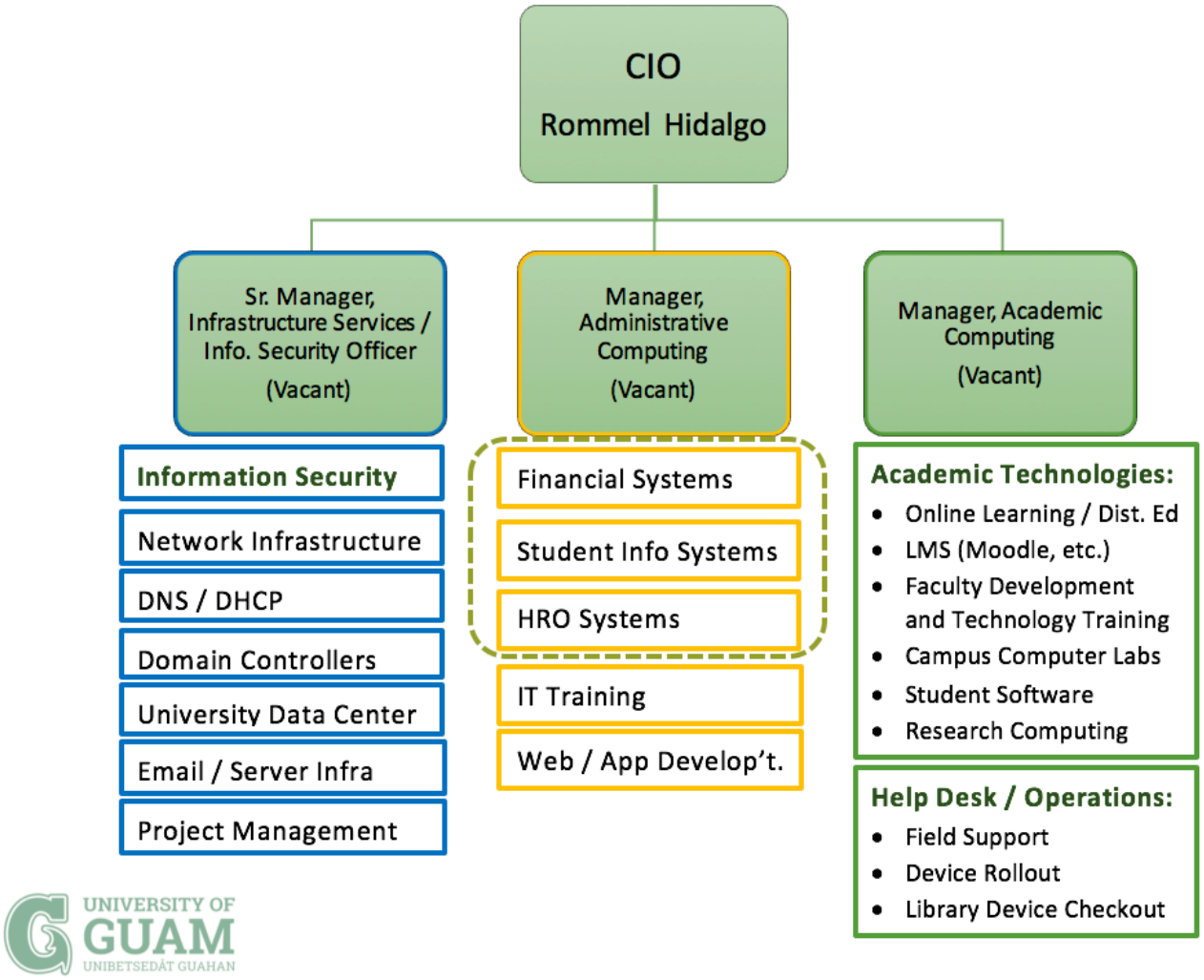

Sr. Executive Team
President Underwood
Sr. Vice President, Acad. & Student Aff.
Vice President, Admin. & Finance
Assistant Vice Presidents
Chief Information Officer
Sr. Manager, Infrastructure Services and Information Security Officer (ISO)
Manager, Administrative Computing
Manager, Academic Computing

Figure 2



At minimum, the Chief Information Officer needs to have three managers/directors reporting to the position to guide the implementation of tasks and projects aligned with G2G and campus-wide IT strategic goals. The three managers/directors are: 1) a Sr. Manager, Infrastructure Services and Information Security Officer; 2) a Manager of Administrative Computing; and 3) a Manager/Director of Academic Computing.

The **Sr. Manager of Infrastructure Services and Information Security Officer** will work with the CIO to implement cyberinfrastructure and cybersecurity technologies, goals, policies, and functionality that will become critical to the institution once it gets Research and Education Network (REN) connectivity. As the university connects to advanced high-speed networks, it must ensure that confidential data maintained by the campus are protected by utilizing industry best practices.

The IT Infrastructure Services and Information Security department will be directly responsible for addressing the institution's **G2G-Connectivity** issue and will strive to achieve the goals established by the University's Information Technology Advisory Committee and Sub-Committees.

The **Manager of Administrative Computing** will ensure that all Enterprise Resource Planning (ERP) systems provide the functions and features needed by the administrative and academic community. The ERP director will work with the CIO to lead institutional efforts to maintain, operate, support, and enhance the critical Financial, Student, and Human Resource Systems. All university operational activities rely on the availability, functionality, and proper maintenance of these campus ERP systems. If the University of Guam decides to continue using Ellucian Colleague as its ERP, the director for this area must implement strategies for quality ERP support and upgrade plans that will enable the system to continue to meet the university's current and future operational needs.

The institutional **G2G-Big Data** issue will be addressed largely by the IT Administrative Computing department. This team will enhance the features and functionality of the Ellucian Colleague ERP; convert paper processes into electronic workflows; automate processes if possible; expand the reporting capabilities of the CROA Big Data system; and actively work to find synergies and efficiencies through enhancements or upgrades of the enterprise systems.

The **Manager of Academic Computing** and the CIO must work with the campus community to strategically develop an academic computing infrastructure capable of supporting **5,000 online students by 2025**. Strategic decisions need to be made regarding the Learning Management System (and other systems) that will be used now and in the future to enable effective teaching and learning. Online students need different resources and support than on-campus students. These online resources and support need to be available anytime, anyplace, anywhere, all year long.

Like students, online faculty will need anytime anyplace, anywhere access to their resources and support systems. Online instructional activities need to be able to work as expected all the time. Additionally, the academic support IT infrastructure needs to do more than just provide help for the LMS, it needs to include a faculty development center designed to keep faculty up to date with the latest technologies and pedagogies relevant to their disciplines, whether they are teaching online or in-person. New active learning methods, classrooms, techniques, and technologies should be made available to faculty and students to pilot test and, in the process, discover new, innovative ways for teaching and learning online and in person.

The IT Department of Academic Computing will need to be daring and lead the campus effort to innovate. Under the CIO's direction, the department will be expected to constantly introduce new academic technologies, concepts, and ideas while providing the guidance and support needed by the Schools and Colleges, to demonstrate what can be achieved through the effective use of technology.

1.10.3 FEEDBACK

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630
HelpDesk: (671) 735-2630
Email: helpdesk@triton.uog.edu
Website: https://it.uog.edu

1.15 | Information Technology Governance @ University of Guam

Effective Date: 08/13/2018 | **Revised Date**: None

1.15.1 IT GOVERNANCE @ UOG

The IT Advisory Committee for the University of Guam is the campus-wide body responsible for providing strategic, technical, and operational Information Technology advice to the CIO and campus senior leadership. The advisory committee will provide strategic leadership, establish campus-wide IT priorities and policies, and ensure transparency and accountability to the University Community with regards to all IT activities on campus. Additionally, the committee will ensure that the campus IT strategic goals and efforts are aligned with the university G2G strategic plan and goals.

This section supersedes the policies set forth in the **University of Guam RRPM manual**, specifically, **Article II. G. 1. g. University Information Technology Committee**.

1.15.2 INFORMATION TECHNOLOGY GOVERNANCE MEMBERSHIP

Information Technology touches all areas on campus. As such, the composition of the Information Technology (IT) Advisory Committee needs to be inclusive to ensure that all stakeholders have a voice in the strategies, goals, and priorities recommended and set by the committee. The IT Advisory Committee, in consultation with the Academic Officers' Council, the Administrative Council, and the Senior Executive Team shall be responsible for overseeing changes in the makeup of the IT Advisory Committee and communicating any changes or additions to appropriate University of Guam stakeholders.

1.15.2.1 COMPOSITION OF IT ADVISORY COMMITTEE. The makeup of the IT Advisory Committee shall be updated by the IT Advisory Committee as necessary to reflect changes in the University's academic, administrative, or technical environments, or applicable laws and regulations.

The current composition of the IT Advisory Committee is as follows:

- **Co-Chairs**
  - Chief Information Officer
  - Rotates annually between the Senior Vice President for Academic and Student Affairs and the Vice President for Administration and Finance
- **Academic Affairs**
  - Director, MARC and RFK Library
  - Dean, Enrollment Management and Student Success
  - Director, Financial Aid Office
  - Director, Professional and International Programs
  - The Dean from each of the Schools and Colleges listed below, or one (1) faculty member appointed for a two (2) year term from each College by the Dean thereof:
    - CLASS; CNAS; SBPA; SNHS; Library; SENG
- **Student Government Association**
  - SGA President or Proxy
- **Administration and Finance**
  - Vice President for Administration and Finance or Proxy
  - Chief Plant and Facilities Officer or Proxy
- **President's Office**
  - Director, Integrated Marketing and Communications or Proxy
- **Endowment Foundation**
  - Executive Director, UOG Endowment Foundation or Proxy
- **Ex-Officio: Office of Information Technology**
  - Office of IT Administrators
  - 2-3 Office of IT Technical Staff

1.15.3 INFORMATION TECHNOLOGY GOVERNANCE SUB-COMMITTEES

There will be four sub-committees that will be responsible for addressing specific campus-wide action items or IT strategic goals. The following sub-committees will report up to the IT Advisory Committee regarding IT policies, tasks, or project outcomes and statuses: 1) **Academic Computing and UOG Online** Sub-Committee; 2) **Administrative Computing** Sub-Committee; 3) **Information Security** Sub-Committee; 4) **Web Presence** Sub-Committee.

1.15.3.1 COMPOSITION OF IT ADVISORY SUB-COMMITTEES. The makeup and annual goals of the IT Advisory Sub-Committees shall be updated by each IT Advisory Sub-Committee and submitted to the IT Advisory Committee for approval. These revisions will be completed as necessary to reflect changes in the University's academic, administrative, or technical environments, or applicable laws and regulations.

1.15.3.1.1 OVERVIEW, CHARGE, AND COMPOSITION OF **IT ACADEMIC COMPUTING AND UOG ONLINE SUB-COMMITTEE**.

The IT Academic Computing and UOG Online Sub-Committee for the University of Guam will strategically develop an academic computing infrastructure capable of supporting up to 5,000 online students by 2025. This IT sub-committee will push forward the strategic decisions that need to be made regarding the Learning Management System and other systems that will be used now and in the future to enable effective teaching and learning. Online students need different resources and support than on-campus students. These online resources and support need to be available anytime, anyplace, anywhere, all year long.

This sub-committee will be the campus-wide body responsible for providing strategic, technical, and operational academic computing advice to the UOG IT Advisory Committee. This sub-committee will establish campus-wide IT academic computing priorities and policies, and ensure transparency and accountability to the university community with regards to all IT academic computing activities on campus. Finally, the committee will ensure that the IT academic computing strategic goals and efforts are aligned with the university G2G strategic plan and goals.

The composition of the IT Academic Computing and UOG Online Sub-Committee needs to be inclusive to ensure that all stakeholders have a voice in the strategies, goals, policies, and priorities recommended and set by the committee.

The current composition of the IT Academic Computing and UOG Online Sub-Committee is as follows:

- **Chair (2-year term, voted by members of the Sub-Committee)**
  - Acting Director, MARC and RFK Library
- **Academic Affairs**
  - Director, Professional and International Programs
  - Assoc. Director, TADEO or Proxy
  - Director, RFK Library or Proxy
  - Faculty Senate Representative
  - EPSCoR Grant Project Representative
  - Water and Environmental Research Institute Representative
  - Assistant VP for Academic Excellence
  - Assistant VP for Institutional Effectiveness
- **Dean's Council**
  - CLASS Dean or Faculty Representative
  - CNAS Dean or Faculty Representative
  - SBPA Dean or Faculty Representative
  - SOE Dean or Faculty Representative
  - School of Engineering Dean or Faculty Representative
  - SNHS Dean or Faculty Representative
- **Student Government Association**
  - SGA Student Representative

- **Administration and Finance**
  - Associate Budget and Program Officer
- **Research Corporation of the University of Guam**
  - Executive Director, RCUOG or Proxy
- **Ex-Officio: Office of Information Technology**
  - Chief Information Officer
  - Manager, Administrative Computing
  - Manager / Director, Academic Computing
  - 2-3 Office of IT Technical Staff

1.15.3.1.2 OVERVIEW, CHARGE, AND COMPOSITION OF **IT ADMINISTRATIVE COMPUTING SUB-COMMITTEE**.

The IT Administrative Computing Sub-Committee will be the campus-wide body responsible for providing strategic, technical, and operational advice to the UOG IT Advisory Committee. This advisory sub-committee will establish campus-wide IT administrative computing priorities and policies, and ensure transparency and accountability to the University Community with regards to all IT administrative computing activities on campus. Additionally, the committee will ensure that the campus IT strategic goals and efforts are aligned with the university G2G strategic plan and goals.

IT Administrative Computing touches all areas on campus. As such, the composition of the IT Administrative Computing Sub-Committee needs to be inclusive to ensure that all stakeholders have a voice in the strategies, goals, and priorities recommended and set by the committee.

The current composition of the IT Administrative Computing Sub-Committee is as follows:

- **Chair (2-year term, voted by members of the Sub-Committee)**
  - Acting Dean, Enrollment Management and Student Success
- **Administration and Finance**
  - Associate University Comptroller
  - Chief Human Resources Officer
  - Supply Management Administrator
  - Associate Budget and Program Officer
- **Academic Affairs**
  - Director, RFK Library
  - Director, Financial Aid Office
  - Director, Admissions and Records Office
  - Dean's Council Representative
- **Student Government Association**
  - SGA Student Representative
- **Research Corporation of the University of Guam**
  - Chief Business Officer, RCUOG or Proxy
- **UOG Endowment Foundation**
  - Executive Director, UOG Endowment Foundation or Proxy
- **President's Office**
  - Director, Integrated Marketing and Communications
  - Director, Development and Alumni Affairs
- **Ex-Officio: Office of Information Technology**
  - Chief Information Officer
  - Manager, Infrastructure Services and Information Security Officer
  - Manager, Administrative Computing
  - Manager / Director, Academic Computing
  - 2-3 Office of IT Technical Staff

1.15.3.1.3 OVERVIEW, CHARGE, AND COMPOSITION OF **IT INFORMATION SECURITY SUB-COMMITTEE**.

The IT Information Security Sub-Committee will be the campus-wide body responsible for providing strategic, technical, and operational information security advice to the UOG IT Advisory Committee. This sub-committee will establish campus-wide IT information security priorities and policies, and ensure transparency and accountability to the university community with regards to all IT information security activities on campus. Additionally, the committee will ensure that the campus IT strategic goals and efforts are aligned with the university G2G strategic plan and goals.

IT Information Security touches all areas on campus. As such, the composition of the IT Information Security Sub-Committee needs to be inclusive to ensure that all stakeholders have a voice in the strategies, goals, and priorities recommended and set by the committee.

The current composition of the IT Information Security Sub-Committee is as follows:

- **Chair**
  - Manager, Infrastructure Services and Information Security Officer
- **Administration and Finance**
  - University Comptroller
  - Associate University Comptroller
  - Chief Human Resources Officer
- **Academic Affairs**
  - Director, Admissions and Records Office
  - Director, Financial Aid Office
  - Dean's Council Representative
- **Three (3) Representatives from the Dean's Council selected by the Dean's Council to serve 2-year terms.**
- **Student Government Association**
  - SGA Student Representative
- **Research Corporation of the University of Guam**
  - Chief Business Officer, RCUOG or Proxy
- **UOG Endowment Foundation**
  - Executive Director, UOG Endowment Foundation or Proxy
- **President's Office**
  - Director, Integrated Marketing and Communications
  - Director, Development and Alumni Affairs
- **Ex-Officio: Office of Information Technology**
  - Chief Information Officer
  - Manager, Infrastructure Services and Information Security Officer
  - Manager, Administrative Computing
  - Manager / Director, Academic Computing
  - 2-3 Office of IT Technical Staff

1.15.3.1.3 OVERVIEW, CHARGE, AND COMPOSITION OF **IT WEB PRESENCE SUB-COMMITTEE**.

The University Web Presence Sub-Committee will be the campus-wide body responsible for providing strategic, technical, and operational web presence advice to the UOG IT Advisory Committee. This sub-committee will establish university web presence priorities and policies, and ensure transparency and accountability to the university community with regards to all university web presence activities and standards on campus. Additionally, the committee will ensure that the campus IT strategic goals and efforts are aligned with the university G2G strategic plan and goals.

University Web Presence touches all areas on campus. As such, the composition of the University Web Presence Sub-Committee needs to be inclusive to ensure that all stakeholders have a voice in the strategies, goals, and priorities recommended and set by the committee.

The current composition of the IT Web Presence Sub-Committee is as follows:

- **Chair**
  - Director, Integrated Marketing and Communications
- **Administration and Finance**
  - Bursar's Office Representative
  - Triton Bookstore Representative
  - Professional and International Programs Representative
  - Human Resources Office Representative
- **Academic Affairs**
  - CNAS Representative
  - CLASS Representative
  - TADEO, OLL Representative
  - CEDDARS Representative, Disability Media Specialist
  - Dean, EMSS or Proxy
  - RFK Library Representative
- **Student Government Association**
  - SGA Student Representative
- **Ex-Officio: Office of Information Technology**
  - Chief Information Officer or Proxy
  - Manager, Infrastructure Services and Information Security Officer
  - 2-3 Office of IT Technical Staff

1.15.4 FEEDBACK

1.15.4.1 University faculty, staff, students, administrators, or other authorized users may provide feedback about this policy through our contact information below:

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630
HelpDesk: (671) 735-2630
Fax: (671) 734-9422
Email: helpdesk@triton.uog.edu
Website: https://it.uog.edu

2.00 | Responsible Use Policy

Effective Date: 08/13/2018 | **Revised Date**: 08/13/2018

2.00.1 POLICY OBJECTIVE

The University of Guam (UOG) provides access to information assets for purposes related to its mission and to the responsibilities and necessary activities of its faculty, students, and staff. These resources are vital for the fulfillment of the academic, research and business needs of the UOG community. This policy defines user, system administrator and UOG responsibilities with respect to the use of UOG information assets.

2.00.2 POLICY STATEMENT

Introduction

The University of Guam (UOG) provides access to information assets for purposes related to its mission and to the responsibilities and necessary activities of its faculty, students, and staff. These resources are vital for the fulfillment of the academic, research and business needs of the UOG community. This policy defines user, system administrator and UOG responsibilities with respect to the use of UOG information assets.

The UOG regards the principle of academic freedom to be a key factor in ensuring the effective application of this policy. The University of Guam is a U.S. accredited, regional Land-Grant institution. It is dedicated to the search for and dissemination of knowledge, wisdom and truth. The University exists to service its learners and the communities of Guam, Micronesia and the neighboring regions of the Pacific and Asia. The University prepares learners for life by providing the opportunity to acquire knowledge, skills, attitudes, and abilities through the core curriculum, degree programs, research and outreach. At the Pacific crosscurrents of the East and West, the University of Guam provides a unique opportunity to acquire indigenous and global knowledge.

Academic freedom is at the heart of a university's fundamental mission of discovery and advancement of knowledge and its dissemination to students and the public. UOG is committed to upholding and preserving the principles of academic freedom: the rights of faculty to teach, conduct research or other scholarship, and publish free of external constraints other than those normally denoted by the scholarly standards of a discipline.

This policy is intended to define, promote, and encourage responsible use of UOG information assets among members of the UOG community. This policy is not intended to prevent, prohibit, or inhibit the sanctioned use of UOG information assets as required to meet the UOG's core mission and campus academic and administrative purposes.

The requirements stated within this policy must not be taken to supersede or conflict with applicable laws, regulations, collective bargaining agreements or other UOG and campus policies.

2.00.3 SCOPE

2.00.3.1 It is the collective responsibility of all users to ensure the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the UOG and to use UOG assets in an effective, efficient, ethical, and legal manner.

2.00.3.2 The UOG RESPONSIBLE USE POLICY shall apply to the following:

a) Central and departmentally managed campus information assets.
b) All users employed by campuses or any other person with access to campus information assets.

c) All categories of information, regardless of the medium in which the information as set is held or transmitted (e.g. physical or electronic).
d) Information technology facilities, applications, hardware systems, and network resources owned or managed by the UOG.

2.00.3.3 Auxiliaries, external businesses and organizations that use UOG information assets must comply with the UOG RESPONSIBLE USE POLICY.

2.00.4 POLICY MANAGEMENT

2.00.4.1 The UOG RESPONSIBLE USE POLICY shall be updated as necessary to reflect changes in the UOG's academic, administrative, or technical environments, or applicable laws and regulations. The UOG Chief Information Security Officer shall be responsible for overseeing a periodic review of this policy and communicating any changes or additions to appropriate UOG stakeholders.

2.00.4.2 The policy may be augmented, but neither supplanted nor diminished, by additional policies and standards adopted by each division or unit.

2.00.4.3 Each division or unit, through consultation with campus officials and key stakeholders, must develop policies, standards, and implementation procedures referenced in the UOG RESPONSIBLE USE POLICY.

2.00.5 GENERAL PRINCIPLES

2.00.5.1 The purpose of these principles is to provide a frame of reference for user responsibilities and to promote the ethical, legal, and secure use of UoG resources for the protection of all members of the UoG community.

2.00.5.2 Use of UoG information assets shall be consistent with the education, research, and public service mission of the UoG, applicable laws, regulations, and UoG/campus policies.

2.00.5.3 All users (e.g., faculty, staff, students, third parties) are required to comply with UoG and campus policies and standards related to information security.

2.00.5.4 All users (e.g., faculty, staff, students, business partners) are required to help maintain a safe computing environment by notifying appropriate UoG officials of known vulnerabilities, risks, and breaches involving UoG information assets.

2.00.5.5 It is the policy of the UoG to make information assets and services accessible in order to meet the needs of UoG students, faculty, staff, and the general public.

2.00.5.6 All users, including those with expanded privileges (e.g., system administrators and service providers), shall respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics, and video.

2.00.5.7 The UoG respects freedom of expression in electronic communications on its computing and networking systems. Although this electronic speech has broad protections, all University community members are expected to use the information technology facilities considerately with the understanding that the electronic dissemination of information may be available to a broad and diverse audience including those outside the university.

2.00.5.8 Other than publicly designated official UoG sites, the UoG does not generally monitor or restrict content residing on UoG systems or transported across its networks; however, the UoG reserves the right to use appropriate means to safeguard its data, preserve network and information system integrity, and

ensure continued delivery of services to users. These activities are not intended to restrict, monitor, or use the content of legitimate academic and organizational communications.

2.00.5.9 In the normal course of system and information security maintenance, both preventive and troubleshooting, system administrators and service providers may be required to view files and monitor content on the UoG and campus networks, equipment, or computing resources. These individuals shall maintain the confidentiality and privacy of information unless otherwise required by law or UoG/campus policy.

2.00.5.10 The UoG recognizes and acknowledges employee incidental use of its computing and network resources within the guidelines defined in the "Incidental Use" section of this policy, at paragraph 4.4 below.

2.00.5.11 All investigations of UoG or campus policy violations, non-compliance with applicable laws and regulations or contractual agreements will be conducted in accordance with appropriate UoG and campus procedures.

2.00.6 USER RESPONSIBILITIES

This section describes user responsibilities governing access, responsible use, network and information system integrity, and incidental use. These statements are not designed to prevent, prohibit, or inhibit faculty and staff from fulfilling the mission of the UoG. Rather, these statements are designed to support an environment for teaching and learning by ensuring that UoG resources are used appropriately.

2.00.6.1 Responsible Use of Information Assets

2.00.6.1.1 Users are expected to use good judgment and reasonable care in order to protect and preserve the integrity of UoG equipment, its data and software, and its access.

2.00.6.1.2 Users must not use or access UoG information assets in a manner that:

a) Conflicts with the UoG mission;
b) Violates applicable laws, regulations, contractual agreements, UoG/campus policies or standards; or
c) Causes damage to or impairs UoG information assets or the productivity of UoG users through intentional, negligent, or reckless action.

2.00.6.1.3 Users must take reasonable precautions to avoid introducing harmful software, such as viruses, into UoG computing and networking systems.

2.00.6.1.4 Unless appropriately authorized, users must not knowingly disable automated update services configured on UoG computers.

2.00.6.1.5 Users must take reasonable precautions to ensure their personal and/or UoG-provided devices (e.g., computers, tablets, smart phones) are secure before connecting to UoG information assets.

2.00.6.1.6 Users must close or secure connections to UoG information assets (e.g. remote desktop, virtual private network connections) once they have completed UoG-related activities or when the asset is left unattended.

2.00.6.1.7 Users must promptly report the loss or theft of any device, which grants physical access to a UoG facility (e.g., keys, access cards or tokens), or electronic access (passwords or other credentials) to UoG resources.

2.00.6.1.8 Users who publish or maintain information on UoG information assets are responsible for ensuring that information they post comply with applicable laws, regulations, and UoG/campus policies concerning copyrighted material and fair use of intellectual property.

2.00.6.1.9 Software must be used in a way that is consistent with the relevant license agreement. Unauthorized copies of licensed or copyrighted software may not be created or distributed.

2.00.6.1.10 A user who has knowledge (or reasonable suspicion) of a violation of this policy must follow applicable UoG and campus procedures for reporting the violation. A user must not prevent or obstruct another user from reporting a security incident or policy violation.

2.00.6.2 Prohibition Against Unauthorized Browsing and Monitoring

2.00.6.2.1 The UoG supports and protects the concepts of privacy and protects the confidentiality and integrity of personal information maintained in educational, administrative, or medical records. Information stored in UoG information systems may be subject to privacy laws.

2.00.6.2.2 Users must not browse, monitor, alter, or access email messages or stored files in another user's account unless specifically authorized by the user. However, such activity may be permitted under the following conditions:

a) The activity is permitted under UoG or campus policy.
b) The activity is defined in the user's job description.
c) The activity is conducted under the authority and supervision of an approved UoG official acting within his or her job responsibilities.
d) The activity is part of a classroom exercise conducted under the supervision of a faculty member. In this case, the faculty member must ensure the exercise does not result in a breach of confidentiality, availability, and integrity of UoG information assets.
e) The activity is conducted to comply with an applicable law, regulation, or under the guidance of law enforcement or legal counsel.

2.00.6.3 Responsibility of Account Owners

2.00.6.3.1 The owner or custodian of credentials, such as a username and password, that permit access to a UoG information system or network resource is responsible for all activity initiated by the user and performed under his /her credentials. The user shall assist in the investigation and resolution of a security incident regardless of whether or not the activity occurred without the user's knowledge and as a result of circumstances outside his or her control.

2.00.6.3.2 Users must take reasonable steps to appropriately protect their credentials from becoming known by, or used by others.

a) Users who have been authorized to use a password-protected account must follow established procedures for setting, maintaining, and changing passwords.

*Unless specific prior authorization has been granted, users are **prohibited** from:*

b) Using or attempting to use the account to access, modify, or destroy UoG or non-UoG information assets for which a user is not normally authorized.
c) Disclosing passwords to any party or including passwords in documentation.
d) Embedding passwords in software code.

2.00.6.3.3 With the exception of publicly accessible UoG information assets, users must not transfer or provide access to UoG information assets to outside individuals or groups without proper authorization.

2.00.6.3.4 Users of UoG information assets must not purposefully misrepresent their identity, either directly or by implication, with the intent of using false identities for inappropriate purposes.

2.00.6.3.5 In the few instances where special circumstances or system requirements mandate that multiple users access the same account, extreme care must be used to protect the security of the

account and its access password. Management of this account must conform to written or published UoG procedures designed to mitigate risk associated with shared access accounts.

2.00.6.4 Incidental Use

2.00.6.4.1 University-owned/managed information assets are provided to facilitate a person's essential work as an employee, student, or other role within the University. Use of university owned computer systems for University-related professional development or academic activities such as research or publication is permitted within the limits of system capacities.

2.00.6.4.2 Personal use of UoG information assets must be no more than "de minimis " (e.g. must have so little value that accounting for it would be unreasonable or impractical). Individuals may use UoG information assets for occasional incidental and minimal personal use provided such use:

a) Does not violate applicable laws
b) Is not in pursuit of the individual's private financial gain or advantage.
c) Does not interfere with the operation or maintenance of University information assets.
d) Does not interfere with the use of University information assets by others.
e) Does not interfere with the performance of the assigned duties of a university employee.
f) Does not result in a loss to the University.

2.00.7 UOG RESPONSIBILITIES

2.00.7.1 The UoG has broad responsibilities with respect to protecting its information assets. These include, but are not limited to controlling access to information, responding to and addressing information security incidents, complying with laws and regulations, and ensuring the logical and physical security of the underlying technology used to store and transmit information.

2.00.7.2 The UoG retains ownership or stewardship of information assets owned (or managed) by or entrusted to the UoG. The UoG reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include but is not limited to: monitoring communications across network services; monitoring actions on information systems; checking information systems attached to the network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from information systems and across network resources. These activities are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

2.00.8 POLICY ENFORCEMENT

2.00.8.1 The UoG respects the rights of its employees and students. In support of the UoG Information Security policies, the campus will establish procedures that ensure investigations involving employees and students suspected of violating the UoG Information Security policy are conducted. These procedures must comply with appropriate laws, regulations, collective bargaining agreements, and UoG campus policies. Additionally, the campus must develop procedures for reporting violations of this policy.

2.00.8.2 The UoG reserves the right to temporarily or permanently suspend, block, or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of UoG resources or to protect the UoG from liability. Suspension, block, or restriction to information assets in such a manner as to substantially affect the ability to complete assigned coursework or job duties shall be considered disciplinary actions subject to paragraph 8.3 below.

2.00.8.3 Allegations against employees that are sustained may result in disciplinary action. Such actions must be administered in a manner consistent with the following:

- The terms of applicable collective bargaining agreement(s).
- The Guam Code Annotated Title 17: Education, Division 3 – University of Guam.
- Other pertinent Guam laws that are applicable to the situation and Informaton Securty infraction.
- The Personnel Rules and Regulations of Government of Guam employees.
- The Personnel Rules and Regulations of the University of Guam.

Student infractions of UoG Information Security policies must be handled in accordance with the established student conduct process.

Auxiliary employees who violate the UoG policies may be subject to appropriate disciplinary actions as defined by their organization's policies.

Third party service providers who do not comply with UoG policies may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the UoG.

2.00.8.4 The UoG may also refer suspected violations to appropriate law enforcement agencies.

2.00.9 FEEDBACK

2.00.9.1 University faculty, staff, students, administrators, or other authorized users may provide feedback about this policy through our contact information below:

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630
HelpDesk: (671) 735-2630
Fax: (671) 734-9422
Email: helpdesk@triton.uog.edu
Website: https://it.uog.edu

2.50 | Information Security Policy

Effective Date: 08/13/2018 | **Revised Date**: None

2.50.1 INFORMATION SECURITY POLICY

The University of Guam has implemented a separate, comprehensive, Information Security University Policy Manual (InfoSec-UPM). **Please refer to the InfoSec-UPM document for all Policies, Regulations and Procedures regarding Information Security at the University of Guam.**

2.60 | Information Security Data Classification Standards

Effective Date: 08/13/2018 | **Revised Date**: 08/13/2018

2.60.1 INTRODUCTION

This document describes the three levels of data classification that the University has adopted regarding the level of security placed on the particular types of information assets. The three levels described below are meant to be illustrative, and the list of examples of the types of data contained below is not exhaustive. Please note that this classification standard is not intended to be used to determine eligibility of requests for information under FERPA or HEERA. These requests should be analyzed by the appropriate legal counsel or administrator.

Classification Description: Level 1 - Confidential

Access, storage and transmissions of Level 1 Confidential information are subject to restrictions as described in UOG Asset Management Standards.

Information may be classified as confidential based on criteria including but not limited to:

a) Disclosure exemptions - Information maintained by the University that is exempt from disclosure under the provisions of the Guam Code Annotated Title 5: Government Operations, Division 1, Chapter 10 – Freedom of Information (Sunshine Reform Act), or other applicable Government of Guam or federal laws.

b) Severe risk - Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the UOG, its students, employees, or customers. Financial loss, damage to the UOG's reputation, and legal action could occur.

c) Limited use - Information intended solely for use within the UOG and limited to those with a "business need-to know."

d) Legal Obligations - Information for which disclosure to persons outside of the University is governed by specific standards and controls designed to protect the information.

Examples of Level 1 – Confidential information include but are not limited to:

- *Passwords or credentials that grant access to level 1 and level 2 data*
- *PINs (Personal Identification Numbers)*
- *Birth date combined with last four digits of SSN and name*
- *Credit card numbers with cardholder name*
- *Tax ID with name*
- *Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name*
- *Social Security number and name*
- *Health insurance information*
- *Medical records related to an individual*
- *Psychological Counseling records related to an individual*
- *Bank account or debit card information in combination with any required security code, access code, or password that would permit access to an individual's financial account*
- *Biometric information*
- *Electronic or digitized signatures*
- *Private key (digital certificate)*
- *Law enforcement personnel records*
- *Criminal background check result*

Classification Description: Level 2 – Internal Use

Access, storage and transmissions of Level 2 - Internal Use information are subject to restrictions as described in UOG Asset Management Standard.

Information may be classified as "internal use" based on criteria including but not limited to:

a) Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations.

b) Moderate risk - Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the UOG's reputation, violate an individual's privacy rights, or make legal action necessary.

Examples of Level 2 – Internal Use information include but are not limited to:

- *Identity Validation Keys (name with)*
  - *Birth date (full: mm-dd-yy)*
  - *Birth date (partial: mm-dd only)*
- *Photo (taken for identification purposes)*
- *Student Information-Educational Records not defined as "directory" information, typically:*
  - *Grades*
  - *Courses taken*
  - *Schedule*
  - *Test Scores*
  - *Advising records*
  - *Educational services received*
  - *Disciplinary actions*
  - *Student photo*
- *Library circulation information.*
- *Trade secrets or intellectual property such as research activities*
- *Location of critical or protected assets*
- *Licensed software*
- *Vulnerability/security information related to a campus or system*
- *Campus attorney-client communications*
- *Employee Information*
  - *Employee net salary*
  - *Home address*
  - *Personal telephone numbers*
  - *Personal email address*
  - *Payment History*
  - *Employee evaluations*
  - *Pre-employment background investigations*
  - *Mother's maiden name*
  - *Race and ethnicity*
  - *Parents' and other family members' names*
  - *Birthplace (City, State, Country)*
  - *Gender*
  - *Marital Status*
  - *Physical description*
  - *Other*

Classification Description: Level 3 - General

Information which may be designated by your campus as publically available and/or intended to be provided to the public.

Information at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of the campus in order to mitigate potential risks.

Disclosure of this information does not expose the UOG to financial loss or jeopardize the security of the UOG's information assets.

REVISION CONTROL

Last Revised:

DRAFT: 04/02/18

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	3/31/2018	Hidalgo	Draft Standard	All
1.1	4/02/2018	Hidalgo	Format draft.	All
1.2	4/02/2018	Hidalgo	Reformat, updates to definitions	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
4/xx/18	Underwood	

2.60.2 FEEDBACK

2.60.2.1 University faculty, staff, students, administrators, or other authorized users may provide feedback about this policy through our contact information below:

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630
HelpDesk: (671) 735-2630
Fax: (671) 734-9422
Email: helpdesk@triton.uog.edu
Website: https://it.uog.edu

2.70 | Information Security Password Policy and Standard

Effective Date: 08/13/2018 | **Revised Date**: 08/13/2018

2.70.1 PURPOSE OF POLICY

The Passwords are an important aspect of computer security and are the first line of protection for a user account. A poorly chosen password or one that is shared, intentionally or unintentionally, may result in the compromise of the confidentiality, integrity, and availability of University of Guam resources. As such, all employees are responsible for taking appropriate steps to create and secure strong passwords.

This standard provides guidance to all users and system administrators regarding the security and management of passwords. It establishes a standard for creation, protection and management of strong passwords.

2.70.2 RELATED UNIVERSITY OF GUAM POLICIES AND STANDARDS

TBD—UNDER REVIEW.

2.70.3 ENTITIES AFFECTED BY THIS STANDARD

This standard applies to all employees who have or are responsible for an account or any form of access that supports or requires a password on any system that resides at the University of Guam, has access to the University of Guam network and related networks, or stores any non-public University of Guam information.

This standard applies to all system administrators responsible for establishing or enabling system password parameters.

2.70.4 DEFINITIONS

This standard applies to all employees who have or are responsible for an account or any form of access that supports or requires a password on any system that resides at the University of Guam, has access to the University of Guam network and related networks, or stores any non-public University of Guam information.

2.70.4.1 **Administrative Information Systems**: Any University information system that supports the storage, retrieval and maintenance of information supporting a major administrative function of the University and any associated administrative data that resides on end-users' local desktop or laptop computers and/or department servers. Administrative information systems do not include systems that directly support the teaching and learning and research activities of the University.

2.70.4.2 **Decentralized System**: Any data system or equipment containing data deemed private or confidential, or which contains mission-critical data, including departmental, divisional and other ancillary system or equipment that is not managed by the Office of Information Technology.

2.70.4.3 **Level 1 Confidential Data**: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable Government of Guam or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the UOG, its students, employees or customers. Financial loss, damage to the UOG's reputation

and legal action could occur if data is lost, stolen, unlawfully shared, or otherwise compromised.

Level 1 data is intended solely for use within the UOG and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information.

Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information. Confidential data must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred.

2.70.4.4 **Level 2 Internal Use Data**: Internal use data is information that must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the UOG's reputation, violate an individual's privacy rights, or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

2.70.4.5 **Level 3 Public Data**: This is information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard. Knowledge of this information does not expose the UOG to financial loss or jeopardize the security of the UOG's information assets.

Publicly available data may still be subject to appropriate University review or disclosure procedures to mitigate potential risks of inappropriate disclosure. A student may exercise the option to consider directory information, which is normally considered public information, as confidential per the Family Educational Rights and Privacy Act (FERPA).

Directory information includes the student's name, address, telephone listing, email address, photograph, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, grade level, enrollment status, degrees, honors and awards received, and the most recent educational agency or institution attended by the student.

For bargaining unit student employees, directory information also includes: the name of the department employing the student, the student employee's telephone listing within the department, the student employee's email address within the department and the student employee's job classification.

2.70.4.6 **Password**: Any secret string of characters that serves as authentication of a person's identity and that may be used to grant or deny access. Passwords are classified as **Level 1 Confidential Data**.

2.70.4.7 **Protected Data**: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

2.70.5 STANDARDS

2.70.5.1 General

Unless otherwise authorized, all users of University information assets must be identified with a unique credential that establishes identity. User credentials must require at least one factor of authentication (e.g., token, password, or biometric devices).

Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization. Users are responsible for keeping their password confidential and for all transactions made using their passwords.

The following provide the foundation for sound password management:

- Passwords should meet or exceed complexity requirements based on the risk.
- Passwords should be changed frequently based on risk. The recommended timeframe for password change frequency will be established below in 2.70.5.5.
- Passwords should be protected from exposure.

2.70.5.2 Password Construction

If passwords are poorly chosen, they can easily be guessed either by a person or a program designed to quickly try many possibilities. A good password is one that is not easily guessed but still easy to remember.

Password strength is determined by a passwords length and its complexity. Users are required to construct their passwords based on the requirements and restrictions indicated below and subject to the constraints of the systems where those passwords reside.

2.70.5.2.1 Password Requirements

All passwords must conform to the following minimum requirements:

- Minimum of 8 characters (longer is generally better)
- At least one character from each of the following:
    - Upper case letters (A-Z)
    - Lower case letters (a-z)
    - Numeric character (0-9)
    - Non-alphanumeric character (all keyboard characters not defined as letters or numerals). Some University systems may not support non-alphanumeric characters or only support a specific subset.
- NOTE to System Administrators
    - If there are system limitations that do not allow for conformance with the above requirements or there is a need for a higher level of security due to the sensitivity of the data, then the responsible system administrator must specify password requirements and a corresponding password change schedule based on the assessment of risk. Also, there may be instances due to contract or research requirements that necessitate more stringent password requirements.

    - System administrators should be aware that some password mechanisms have more limited character sets than users would expect (e.g., an application might permit users to enter mixed case passwords but then convert all lower-case letters to uppercase before hashing the password) or may accept password characters past the maximum length that is stored or checked.

2.70.5.3 Password Restrictions

The password should NOT:

- Use any names, person, places or things found in a dictionary (English or foreign).
- Have more than two characters repeated consecutively.
- Use adjacent keyboard characters as the entire password (e.g., asdfghjkl, qwertyu, 12345678).
- Use public or personnel information such as family names, social security number, user ID, favorite hobbies, TV shows, movie names, credit card or ATM card numbers, telephone number, birth date, driver's license number, license plate numbers, addresses, anniversary date, or pet names.
- Use words, phrases, or acronyms associated with the University (e.g., "GoldenEagle", etc.)

- Use any of the above spelled backwards.
- Use any of the above followed or preceded by a single digit.
- Be so difficult that it is forgotten if not written down.

2.70.5.4 Password Protection

After creating a strong password, it is imperative to keep it confidential.
All users should NOT:

- Enter a password while anyone is watching.
- Write down the user ID and password and then post them on a monitor, telephone or desk, put them under a keyboard or mouse pad, carry them in a wallet or purse, or put them in a PDA device without encryption. If a password must be written down, it should be placed in a secure and private location.
- Use another person's user ID and password.
- Sign on and leave the office without logging off, locking the workstation, or taking other comparable precautions.
- Reveal a password to anyone (e.g., your supervisor, co-worker, family member, etc.) either in person, over the telephone, in an unsecured email message, on questionnaires or security forms.
- Click on a link within an email that asks the recipient to verify a password or other user or account information.
- Hint at the format of a password (e.g., "my family name").
- Use the same password for University business and personal purposes.
- Download and execute files from unknown sources.
- Use administrator-level privileges for daily tasks.

2.70.5.5 Password Change Schedule

TBD—UNDER REVIEW.

2.70.5.6 Password Reuse

Passwords should not be reused. Old passwords may have been compromised or an attacker may have taken a long time to crack encrypted passwords. Reusing an old password could inadvertently give attackers access to the system. University of Guam's Titan Online passwords are controlled by system parameters that disallow password reuse until ten different passwords are used for ten 180-day periods.

2.70.5.7 Compromised Passwords

Passwords that have been or suspected to have been compromised (e.g., stolen, guessed, etc.) should be changed immediately. Immediately report any incidents when you believe someone else is using your password or otherwise accessing your account to IT Security and Compliance at 671-735-2630.

2.70.5.8 Password Transmission

Passwords may be transmitted over internal and external networks to provide authentication capabilities between hosts. The main threat to transmitted passwords is sniffing, which involves using a wired or wireless sniffer to listen to network transmission. Because of sniffing threats, passwords should not be transmitted across untrusted networks without additional encryption unless the passwords have no value and cannot be used to gain access to any significant resources.

Sniffing threats should be mitigated by:

- Encrypting the passwords or the communications containing the passwords.
- Transmitting cryptographic passwords instead of plain text passwords.
- Switching from protocols that do not protect passwords to protocols that do.
- Using network segregation and fully switched networks to protect passwords transmitted on internal networks.
- Replacing a password implementation that exposes the passwords to sniffing with a more secure password-based authentication protocol.

2.70.6 FEEDBACK

2.70.6.1 University faculty, staff, students, administrators, or other authorized users may provide feedback about this policy through our contact information below:

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630
HelpDesk: (671) 735-2630
Fax: (671) 734-9422
Email: helpdesk@triton.uog.edu
Website: https://it.uog.edu

3.00 | University Web Presence Policy

Effective Date: 08/13/2018 | **Revised Date**: None

3.00.1 PURPOSE OF POLICY

The University of Guam Web Presence is currently under development and will be included in the IT-UPM in the next few weeks.

3.10 | University Email Policy

Effective Date: 08/13/2018 | **Revised Date**: 08/13/2018

3.10.1 PURPOSE OF POLICY

Electronic mail (email) shall be considered an appropriate, cost-effective, convenient and timely means to transmit official campus communications. An official communication occurs when an individual or campus entity sends email pertinent to conducting university business for academic or administrative purposes, including notification of university-related actions.

Official communications will be sent to a student's university-assigned email address (**username@gotritons.uog.edu**) or to a staff, faculty, or administrator's university-assigned email address (**username@triton.uog.edu**).

Email may be the sole method for notification. However, additional or other methods of communication will be utilized if appropriate or required by law or other contractual obligations, e.g., notification of disciplinary and legal actions.

Electronic messages sent as official campus communications are expected to comply with applicable laws and campus policies, including those referenced in this policy, and are subject to the same public records, privacy, and records retention requirements and policies as other official campus communications.

University electronic mail and messaging is to be used to enhance and facilitate teaching, learning, scholarly research, support academic experiences, and to facilitate the effective business and administrative processes of the University. It is not to be used for personal or political gain.

This policy is applicable to all users (departments, organizations, individuals) of any University of Guam e-mail system. Users are expected to comply with all applicable laws and university policies affecting the use of email and related systems, including but not limited to responsible use, computer accounts, passwords, information security, and software licensing.

3.10.2 POLICY COMPLIANCE AND OVERSIGHT

The Chief Information Officer (CIO) is responsible for application and enforcement of this policy.

The UoG Information Technology Advisory Committee (ITAC) shall review this policy on an annual basis or as the need arises, make recommendations for any changes, and provide oversight and periodic review of the practices used to implement this policy. Recommended changes shall be reviewed and approved by the CIO in consultation with the ITAC and the President.

The current version of the policy will be posted and maintained on the University of Guam Office of Information Technology website. A hard copy will be available at the RFK Library Reserve Desk.

3.10.3 SPECIFIC PROHIBITIONS

- Altering electronic communications to hide one's identity or to impersonate another individual is considered misrepresentation and/or forgery and is prohibited under this policy. All e-mail, news posts, chat sessions, or any other form of electronic communication must contain the sender's real name and/or e-mail address.

- Initiating or forwarding "chain letters" or e-mail are prohibited on university e-mail systems and the Internet as a whole. Chain e-mail can be identified by phrases such as "please pass this on to your friends" or similar inducements that encourage the recipient to forward the message.

- The practice of bombarding someone with a large volume of unsolicited mail in an attempt to disrupt them or their site is known as "mail bombing". Mail bombs have the effect of seriously degrading system performance and may have legal consequences. This practice is strictly prohibited on UOG systems.

- The practice of sending unsolicited commercial advertisements or solicitations (SPAM) via e-mail is regulated by applicable laws.

    - On-campus users found in violation of these laws could be subject to criminal prosecution, civil prosecution, administrative action, and/or loss of some or all computing privileges.

    - UOG users receiving such messages are responsible for notifying the sender to stop. If the sender refuses to comply or does not provide a valid means for users to be removed from their list, the recipient may take civil action against them. The University will not typically act on the employee's behalf to stop unsolicited email messages.

- Use of electronic communications, including e-mail, with the intent to annoy, harass and/or physically threaten other individuals is prohibited.

- Use of Government of Guam resources, including e-mail, for anyone's personal or political gain is prohibited. This includes promoting off-campus sales and services.

- Operation of unofficial e-mail reflectors is prohibited. An e-mail reflector is the automated or otherwise forwarding of a mail message to multiple recipients triggered by the content or headers of the mail message being forwarded. Authorized reflectors include uog.edu, triton.uog.edu, gotritons.uog.edu and reflectors established by the system administrators of the University machines affected.

- Users are prohibited from sending messages to large numbers of users except as defined in the procedures accompanying this policy. Official mailings to large numbers of users should conform to the "Group Distribution Lists and Broadcast Messages" section of this policy.

- E-mail messages may not include any user's identification number (e.g., social security number), should include only unique identifying information that is pertinent to the message being conveyed, and should not reference any student's academic record or confidential employee information.

- E-mail forwarding is prohibited. Forwarding official emails creates a risk for the university because once emails leave the official university mail server environment, we can no longer control or protect them.

3.10.4 GROUP DISTRIBUTION LISTS AND BROADCAST MESSAGES

Large group mailings are permitted only if sent via authorized distribution methods to reduce the system load. Mailings exceeding the number of addressees specified in the procedures must use system aliases, group distribution lists (DLs) or a system-operated utility. This applies to all inter-machine e-mail as well as campuswide e-mail systems. Examples of system aliases and DLs include class lists, college/department lists (e.g., faculty

and staff rosters), committees, student clubs, other official University organizations, and specific discussion/topic groups.

System aliases and DLs are to be used only for the purpose for which they were created. For example, class aliases are for use by classes in class discussions and dissemination of information within the context of the specified class. Student club aliases are for disseminating official club information. All other aliases are for use by specific units or members to disseminate or share information.

Use of such aliases by non-authorized personnel constitutes a violation of this policy. Official aliases may not be used to broadcast unofficial and/or unauthorized messages. Aliases established to broadcast information may not be used without the express permission of the owner of the list.

For other large group mailings, use of system authorized distribution methods is encouraged, especially when extremely large numbers of users are involved or when the speed with which the message being delivered is not critical.

Messages being "broadcast" to campuswide groups (e.g., all faculty, staff, and/or students) must use an approved broadcast method and meet the following criteria:

- Other means of communication are not timely and the nature of the event was such that timely announcement via other methods could not be accommodated
- An appropriate target audience can be determined
- Could be of significant benefit to all of the targeted audience
- Must comply with applicable university policies on use of State resources
- Prevents significant inconvenience that the lack of the information would cause to the targeted audience
- Must be approved by the president, vice president, or dean
- Must be approved by the Chief Information Officer (CIO) or designee

Units within the university, such as a college or department, may initiate broadcast messages containing official university business to their own constituent groups without seeking the approval of the CIO, but should still observe these criteria. Such mailings should be consistent with the policy, standards, guidelines and procedures.

Broadcast messages should originate from a departmental or unit account, e.g., library, rather than an individual or personal account.

The university reserves the right to perform broadcast mailings which are related to emergencies and university physical plant conditions or activities for which urgent notice is required and that will potentially affect most of the recipients.

3.10.5 CONFIDENTIALITY

E-mail should be avoided as a means of communicating confidential or sensitive material, inasmuch as confidentiality cannot be guaranteed on the Internet.

- It is against university policy for system administrators to monitor the contents of files or messages unless necessary to preserve either system integrity or continued e-mail delivery.

- Moreover, copies of messages are kept on system backups and may be retained for periods of time and locations unknown to you.

- In addition, e-mail messages can be intercepted, copied, read, forged, destroyed, or misused by others for mischievous purposes.

- E-mails, whether or not created or stored on university equipment, may constitute a university record subject to disclosure under the Government of Guam Freedom of Information Act or other laws, or as a result of litigation.

- This includes email-related data stored on a machine's hard drive, regardless of machine ownership.

- Copies of e-mail must be provided in response to a public record request or legally issued subpoena, subject to very limited exceptions, as with all other documents created and retained at the University.

3.10.6 FEEDBACK

3.10.6.1 University faculty, staff, students, administrators, or other authorized users may provide feedback about this policy through our contact information below:

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630
HelpDesk: (671) 735-2630
Fax: (671) 734-9422
Email: helpdesk@triton.uog.edu
Website: https://it.uog.edu

3.50 | University Online Strategy

Effective Date: 08/13/2018 | **Revised Date**: None

3.50.1 PURPOSE OF POLICY

The University of Guam Online Strategy is currently under development and will be included in the IT-UPM in the next few weeks.

4.00 | Guam Open Research & Education eXchange (GOREX)

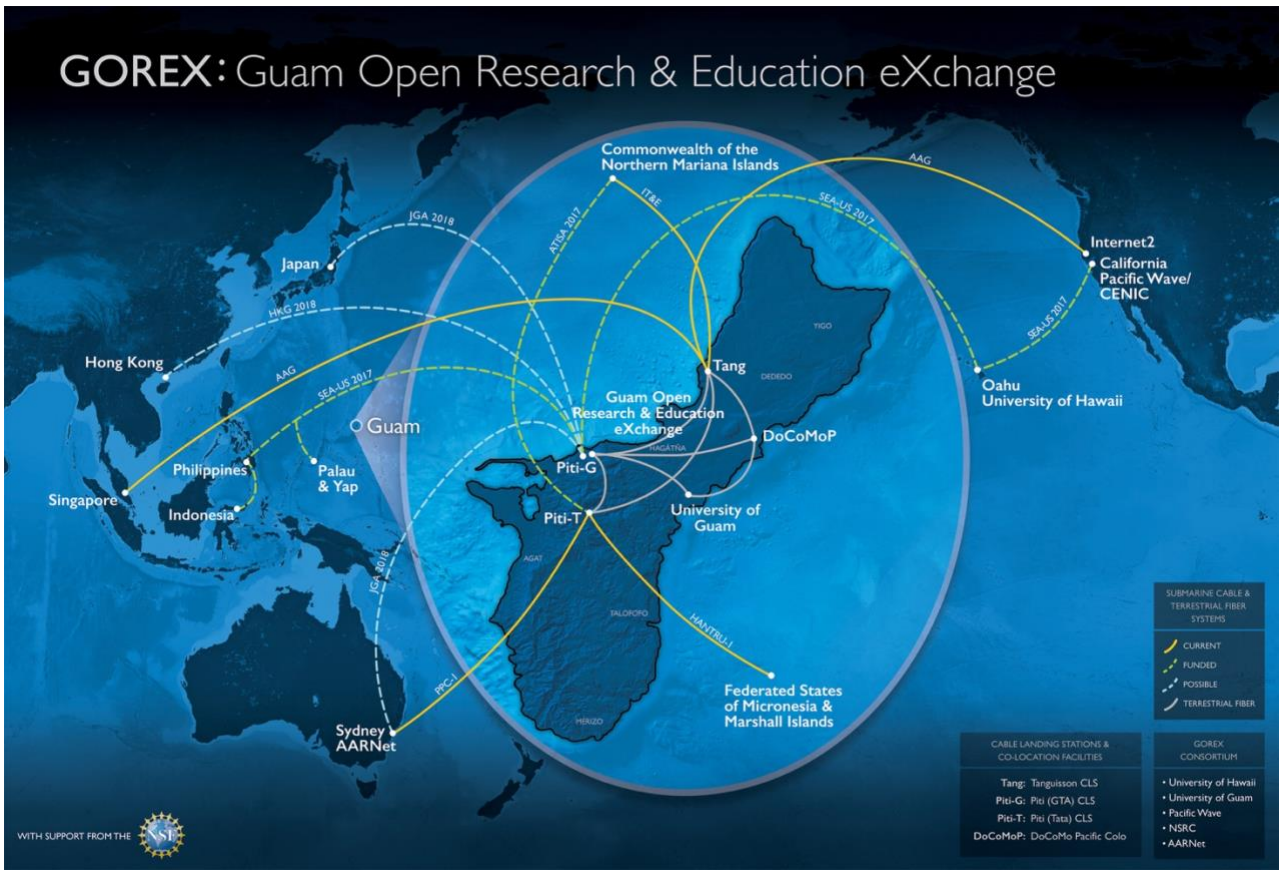
Effective Date: 08/13/2018 | **Revised Date**: None

4.00.1 GUAM OPEN RESEARCH & EDUCATION EXCHANGE (GOREX) CONCEPT

The Guam Open Research and Education eXchange ("GOREX") will leverage the strategic geographic location of Guam and the major new fiber optic systems landing there by establishing an open R&E exchange to inter-connect the existing, funded and planned high capacity R&E trans-Pacific circuits in a planned manner. Specific purposes are to improve Pacific-wide transport diversity and resilience in support of global R&E networks and facilitate greater access to global R&E networks by Pacific Island nations and communities, including Guam itself, by leveraging the multiple regional fiber systems that terminate on Guam. The overarching goal is to promote increased growth and effectiveness of data-intensive and highly collaborative research and education activities engaging the Asia-Pacific region with the global R&E community.

The initial participants in the GOREX consortium will include the University of Hawaii (UH) and Pacific Wave (PWave), the Australia Academic and Research Network (AARNet), Internet2/SingAREN, the University of Guam (UOG), and the NSRC. Additional participation will likely extend to Japan, Hong Kong, and multiple Pacific Islands.

The following diagram portrays this initial concept.



Links portrayed include current, funded and possible connections as follows:

AARNet – Existing path to Singapore via PPC-1 and AAG, currently only transits Guam; Anticipated future higher speed path to Guam over new Japan-Guam-Australia system in 2018,

UH – 100G from Guam to Hawaii and Pacific Wave. Funded with production planned 2017.

SingAREN/Internet2 - Existing 100G path to be AAG/Level3, with likely POP at the DoCoMo

Pacific commercial colocation facility connecting UOG.

Japan (WIDE) – via potential future Japan-Guam-Australia system in 2018,

Hong Kong – Available via potential future Hong Kong – Guam system in 2018.

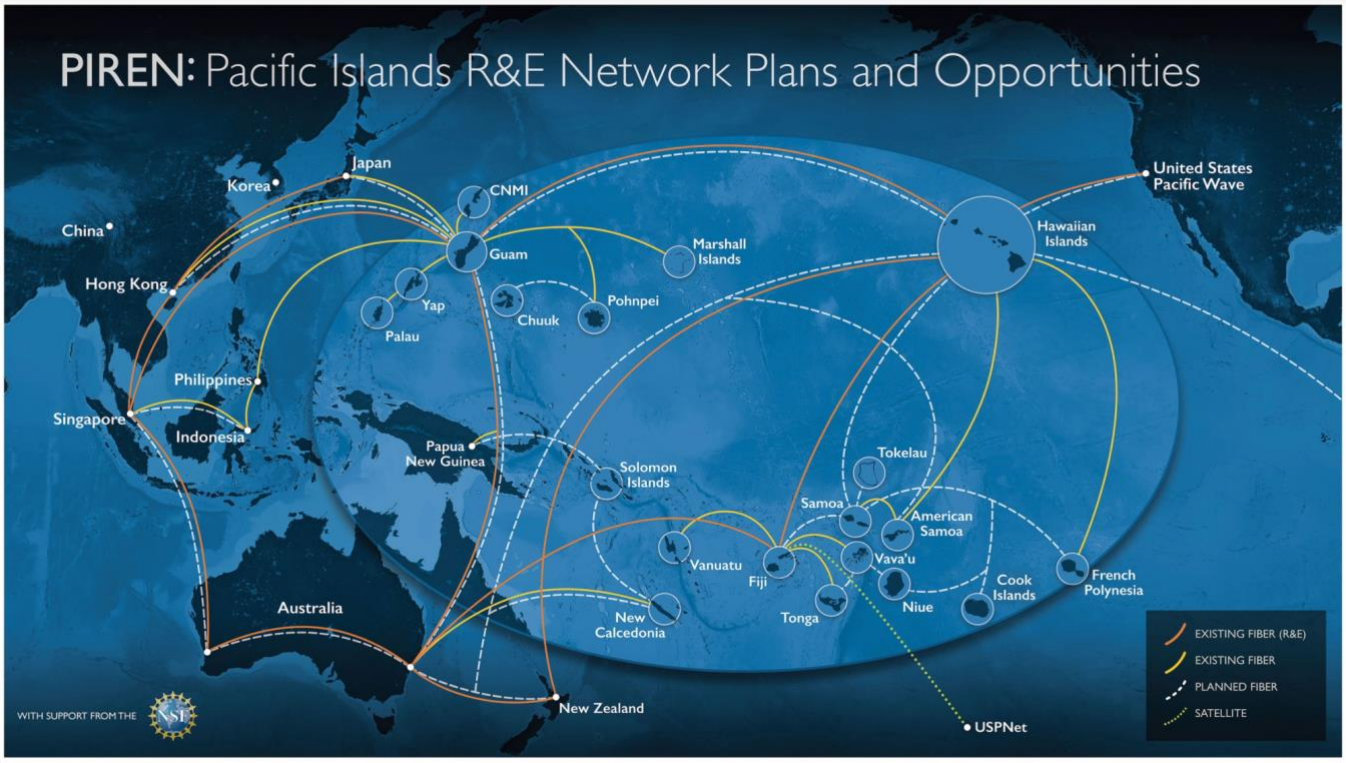
USP/RMI – Available via current AARNet path on HANTRU-1.

College of the Marshall Islands – Available via HANTRU-1.

CNMI – College of the Northern Marianas will be available via ATISA (2017).

Palau and Yap – Available via SEA-US west segment in 2017.

The University of Hawaii will establish the GOREX with all partners as part of its **NSF-funded IRNC PIREN** agreement leveraging PIREN resources with its IRU purchase of new capacity into Guam with State of Hawaii funding. The GOREX will be governed collaboratively with the fundamental principles of providing an open R&E exchange and maximizing value to participants and their respective national and regional R&E networks. We believe that the establishment of the GOX will drive national and regional R&E investment in links to Guam that will result in high value to participants and a more rational and resilient global architecture. The GOX will be operated on a pure non-profit cost-recovery basis with costs shared fairly and transparently among participants. Partners investing in the GOREX, including through the provisioning of substantial submarine fiber connections to the GOREX will provide oversight and lead any governance activities.



Connections to the GOREX may be at Layer 2 or Layer 3, with each organization responsible for the incremental costs of their connection to the GOREX. Depending on the nature of the connection, and the operational standards established for the GOREX by the consortium, connections may be established using organization provided equipment, or via an allocation of a organization-controlled switch port using shared common equipment at the GOREX.

The initial costs to establish and equip the GOREX will be borne by consortium members, to include significant UH investment for startup and with commitments for support from Pacific Wave / CENIC, AARNet, and others. Given the limitations and long-term cost of colocation space and power, dedicated equipment for connections established within the GOREX colocation footprint may be limited to connections at 100G and higher. Connections below 100G will generally be via a switch port on shared common equipment, with exceptions granted for those with material plans to migrate to 100G and higher.

Facilities for the GOREX will include approximately four (4) racks of available colocation space, to be acquired by UH as part of its **SEA-US** IRU purchase. The colocation space will support direct access to any systems that land at the GTA Piti Cable Landing Station (CLS): initially SEA-US and the planned Japan-Guam-Australia and HongKong-Guam systems, along access via terrestrial fiber connections to any of the other Guam CLS facilities -- Piti (Tata), Tumon Bay, Tanguisson – as well as commercial colocation facilities of GTA and DoCoMo Pacific.

For inquiries regarding how to participate in GOREX, please send an email to uognoc@uog.edu.

4.00.2 FEEDBACK

4.002.1 University faculty, staff, students, administrators, or other authorized users may provide feedback about GOREX through our contact information below:

UOG Office of Information Technology
303 University Dr., UOG Station
Computer Center Rm. 104
Mangilao, GU 96913

Main Telephone: (671) 735-2640 / 2630
HelpDesk: (671) 735-2630
Fax: (671) 734-9422
Email: helpdesk@triton.uog.edu
Website: https://gorex.uog.edu

APPENDIX A | GLOSSARY – INFORMATION TECHNOLOGY AND INFORMATION SECURITY

Term	Definition
Anti-virus Software	Software that detects or prevents malicious software.
Application	A software program designed to perform a specific function for a user. Applications include, but are not limited to, word processors, database programs, development tools, image editing programs, and communication programs.
Authentication	The process of confirming that a known individual is correctly associated with a given electronic credential; for example, by use of passwords to confirm correct association with a user or account name (is a term that is also used to verify the identity of network nodes,
Authorized	The process of determining whether or not an identified individual or class has been granted access rights to an information assets, determining what type of access is allowed; e.g., read-only, create, delete, and/or modify.
Availability	Ensuring that information assets are available and ready for use when they are needed.
Biometric Devices	An instrument intended to validate the identity of an individual through comparison of a demonstrated intrinsic physical or behavioral trait with a record of the same information previously captured. Examples: fingerprint,
Business Continuity Planning	See UOG BCP Strategy.
Campus	For the purposes of the UOG Security Program, "campus" is the University of Guam campus and all of its satellite locations.
Campus Limited Access Area	Physical area such as a human resources office, data center, or Network Operations Center (NOC) that has a defined security perimeter such as a card controlled entry door or a staffed reception desk.
Campus Managers	Responsible for (1) specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of program responsibility and (2) ensuring that program staff and other users of the information asset are

	informed of and carry out information security and privacy responsibilities.
Catastrophic Event	An event that causes substantial harm or damage to significant UOG information assets. Examples: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.
Computer Security Incident Response Team (CSIRT)	The name given to the team that handles security incidents.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C, SEC. 3542]
Control	Countermeasures (administrative, physical, and technical) used to manage risks.
Critical Asset	An asset that is so important to the campus that its loss or unavailability is unacceptable.
UOG Network	Any UOG administratively controlled communications network that is within the UOG managed physical space. Such networks may interconnect with other networks or contain sub networks.
Data	Individual facts, statistics, or items of information represented in either electronic or non-electronic forms.
Data Center	A facility used to house information processing or telecommunications equipment that handle protected or critical information assets.
Data Owner	Person identified by law, contract, or policy with responsibility for granting access to and ensuring appropriate controls are in place to protect information assets. The duties include but are not limited to classifying, defining controls, authorizing access, monitoring compliance with UOG/campus security policies and standards, and identifying the level of acceptable risk for the information asset. A Data Owner is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of information within that unit.

Data Steward	(also known as "Data Custodian") An individual who is responsible for the maintenance and protection of the data. The duties include but are not limited to performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in UOG/campus security policies and standards.
DMZ	DMZ (De-Militarized Zone) is a set of one or more information assets logically located outside of a protected network that is accessible from the Internet (open to the world) with limited controlled data
Electronic Media	Electronic or optical data storage media or devices that include, but are not limited to, the following: magnetic disks, CDs, DVDs, flash drives, memory sticks, and tapes.
Employee	Any person who is hired by the UOG to provide services to or on behalf of the UOG and who does not provide these services as part of an independent business.
Encrypted Protocol	An agreed-to secure means of data transmission over a network (wired or wireless).
Encryption	The process of encoding data so that it can be read only by the sender and the intended recipient.
Excessive Authority	Assignment of a single individual to overlapping administrative or management job functions for a critical information asset without appropriate compensating controls such as added reviews or logging.
Hardening	A defensive strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.
Hardware	Physical devices including, but is not limited to, portable and non-portable workstations, laptops, servers, copiers, printers, faxes, and PDAs.
Information Assets	Information systems, data, and network resources to include automated files and databases.

Information Security Program	An organizational effort that includes, but is not limited: to security policies, standards, procedures, and guidelines plus administrative, physical, and technical controls. The effort may be implemented in either a centralized or a decentralized manner.
Information Systems	A combination of hardware, network and other resources that are used to support applications and/or to process, transmit and store data
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]
Least Privilege	A concept of information security by which users and their associated applications execute with the minimum amount of access required to perform their assigned
Logical Access	The connection of one device or system to another through the use of software.
Lockout Time	The amount of time for which logins to an account are disabled. Usually invoked once a threshold of invalid login attempts has been reached.
Malicious Software	Software designed to damage or disrupts information assets.
Mobile Devices	Devices containing electronic UOG data which are easily transported. Such devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), and "smart" phones.
Network Resources	Resources that include, but are not limited to: network devices (such as routers and switches), communication links, and network bandwidth.
Non-public	A service or information intended only for the internal use of the organization.
Notice-triggering Information	Specific items of personal information identified in GCA Title 9, Chapter 46.
Operating System	Software that is primarily or entirely concerned with controlling a computer and its associated hardware, rather than with processing work for users

Personally Identifiable Information	Any information that identifies or describes an individual, including, but not limited to name, Social Security number, physical description, address, phone number, financial matters, medical or employment history (GCA, Title 9, Chapter 46).
Physical Access	Being able to physically touch, use, and interact with information systems and network devices.
Private IP Addresses	Defined by Request for Comment (RFC) 1918 as range of non- routable addresses.
Protected Asset	Information asset containing protected data.
Protected Data	Level 1 and Level 2 data which are defined in the UOG Data Classification Standard. This data has been categorized according to its risk to loss or harm from disclosure.
Public Information	Any information prepared, owned, used or retained by a campus and not specifically exempt from disclosure requirements of the Freedom of Information Act (Government Code Sections 6250- 6265) or other
Remote Access	Any connection from an external, non-campus network to any campus information system, data, or network
Risk	The likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization.
Risk Assessment	A process by which quantitatively and/or qualitatively, risks are identified and the impacts of those risks are determined. The initial step of risk management.
Risk Management	A structured process which identifies risks, prioritizes them, and then manages them to appropriate and
Risk Mitigation	Reduce the adverse effect of an event by reducing the probability of the event occurring and/or limiting the impact of the event if it does occur
Security Awareness	Awareness of security and controls, in non-technical terms, conveyed to motivate and educate users about important security protections that they can either directly control or be subjected to.

Security Incident	An event that results in any of the following: Unauthorized access or modification to the UOG information assets. An intentional denial of authorized access to the UOG information assets. Inappropriate use of the UOG's information systems or network resources. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.
Security Training	Specific technical understanding of how to secure the confidentiality, integrity and availability of applications, operating systems and information assets to prevent or detect security incidents
Screen Filter	An item which can be used to limit the visibility of content displayed on a computer screen to those who are immediately in front of it.
System Administrator	(also known as "System Personnel" or "Service Providers") Individuals, who manage, operate, support campus information systems; or manage networks.
Third Parties	For the purposes of the UOG Security Program, third parties include, but are not limited to, contractors, service providers, vendors, and those with special contractual agreements or proposals of understanding.
Threat	A person or agent that can cause harm to an organization or its resources. The agent may include other individuals or software (e.g. worms, viruses) acting on behalf of the
User	Anyone or any system which accesses the UOG information assets. Individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.
Vulnerability	A flaw within an environment which can be exploited to cause harm.

Asymmetric Cryptosystem	A computer algorithm or series of algorithms which utilize two different keys with the following characteristics • one key signs or decrypts content; • one key verifies or encrypts content; and, • the keys have the property that, even when one key is known, it is computationally infeasible to discover the other key.
Asymmetric Key-Pair	A private key and its corresponding public key in an asymmetric cryptosystem. Public keys can be used to verify a digital signature created with the corresponding private key and to encrypt content.
Digital Certificate	Also known as a public key certificate or identity certificate, a digital certificate is an electronic document which uses a digital signature to bind a public key with an identity, such as the name of a person or an organization and address. The certificate can be used to verify that a public key
Patch (Patching)	The installation of a software update designed to fix problems, improve usability, or enhance performance.
Private Key	The secret key of a key pair used to create a digital signature or decrypt data.
Public Key	The well-known key of a key pair used to verify a digital signature or to encrypt data.
Public Key Cryptography	An encryption method that uses an asymmetric key-pair.
Signature Dynamics	A measurement of the way a person writes his or her signature by hand on a flat surface, binding the measurements to a message through the use of cryptographic techniques.

REFERENCES

Certain sections of the University of Guam Information Technology University Policy Manual (IT-UPM) were adapted from the information technology policies, procedures, standards, best-practices, and guidelines developed at the following institutions and universities:

- Boise State University
- California State Polytechnic University, Pomona
- California State University, Chancellor's Office
- California State University, Fullerton
- California State University, Los Angeles
- Columbia University
- Corporation for Education Network Initiatives in California (CENIC)
- National Institute of Standards and Technology (NIST)
- National Science Foundation
- University of Hawai'i System
- University of Oregon
- University of Portsmouth, Portsmouth, England
- University System of Georgia

Additional references and resources are listed below:

Boise State University's Policy and Procedures Writing Guide
https://policy.boisestate.edu/policy-writing-guide/
(accessed Jan 28, 2018)

Central Queensland University, Australia
Policy and Procedure Template
www.cqu.edu.au%2Fpolicy%2Fsharepoint-document-download%3Ffile_uri%3D%257BBE8380F3-F86D-4C55-AC0D-84A81EAFD6A2%257D%2FPolicy%2520and%2520Procedure%2520Template%2520-%2520with%2520Instructions.docx&usg=AOvVaw3mbf4zxAwoPjtMwPwWrCdv
(accessed Jan 28, 2018)

Cornell University
University Policy Office Glossary and Style Book For Writing Policy Documents
https://www.dfa.cornell.edu/sites/default/files/upo-stylebook.pdf
(accessed Jan 28, 2018)