Office of Public Accountability
Computer Systems Usage and Social Media Policy

I. General Statement of Policy. 1

II. No Expectation of Privacy. 1

III. Use of Personal Computers 2

IV. Staff Responsibilities. 2

V. Discipline. 3

VI. Internet Access. 4

VII. E-Mail 4

VIII. Social Media 4

IX. Resignation of Staff. 5

As of October 2015

I. General Statement of Policy.

These policies apply to all OPA staff and staff access to computers, other electronic data devices and associated systems now available to staff, or to become available in the future, such as computers, email, telephones, voice mail, fax machines, external electronic bulletin boards, the Internet, other on-line services, and other devices and systems in order to conduct government of Guam business.

These policies are adopted to:

- Facilitate the appropriate use of computers, other electronic data devices, and associated systems.
- Enhance the security and integrity of government computers, electronic data devices, and associated systems.
- Protect the data contained within these devices, services, and systems.
- Preserve data for retrieval as necessary or required by government operations, and as required by law or agreement.
- Prevent the use of government computers, other electronic data devices and associated systems for inappropriate or illegal purposes.
- Recognize that employees maintain privacy rights, provided by the Constitution and by law, and these rights shall be preserved in the application of these policies.

The OPA encourages the use of computers, other electronic data devices and associated systems because they provide more efficient and effective communication, problem solving and storage capabilities. These devices and systems are the property of the OPA and their purpose is to facilitate lawful government activities.

With the rapid changing nature of electronic media this policy cannot address every possible situation. Instead, it expresses general guidelines for using computers, other electronic data devices and associated systems (hereinafter referred to as OPA computer systems). When OPA staff are confronted by a situation not covered by these policies or the policies do not clearly apply to a situation, the staff is encouraged to clarify with her or his supervisor.

II. No Expectation of Privacy.

OPA computer systems and the data contained therein are government property. Staff have no expectation of privacy with OPA computer systems, Internet access, email, voice mail, and electronic data or documents produced, stored or located on OPA computers, devices or systems. A personal password issued to staff does not assure or indicate personal privacy.

At any time, the OPA may inspect and monitor OPA computer systems for legitimate government purposes to assure compliance with law, with this policy, and with other government policies.

III. Use of Personal Computers.

OPA staff are not encouraged to use personally-owned computers and electronic devices for government work. Government records may inadvertently become stored in the private device and require access to such devices, solely for the purpose of gaining access to those government records. Staff must obtain approval before using personal devices to do government work.

IV. Staff Responsibilities.

Government property. Employees shall protect and conserve government property and shall not use it for other than authorized activities.

Obey the law. Use government computers, other electronic data devices and associated systems only for legitimate, business related purposes.

Comply with copyright laws. The OPA complies with federal copyright law. Employees may not use software or computer programs in violation of license agreements. Illegal duplication of software, computer programs or other copyrighted materials on government computers, other electronic data devices and associated systems is prohibited.

Software. All software and computer programs available on government computers, other electronic data devices and associated systems are to be used for business purposes. Software and computer programs may not be altered in any way. Only authorized staff are permitted to add or remove hardware, software, programs or applications to OPA computer systems.

Non-government business prohibited. Employees are prohibited from using OPA computer systems for commercial ventures, religious activity or political causes.

Offensive jokes or language prohibited. OPA computer systems may not be used to access, create, display, send or store messages, images, or content that would reasonably be considered offensive or disruptive. Accessing, creating, displaying, sending, or storing sexual comments, jokes or images, racial slurs, or any comments, jokes or images that would offend on the basis of age, disability, gender, race, religion, national origin, sexual preference, or any other classification protected by law is strictly prohibited.

Removal or destruction of data prohibited. The knowing or purposeful removal or destruction of data on OPA computer systems is prohibited. This data comprises official government records and may only be removed or destroyed by authorized OPA staff. If you are unsure as to whether a certain transaction or activity constitutes a violation of this policy, consult your immediate supervisor for clarification.

The accidental removal or destruction of data on OPA computer systems shall be reported immediately to your supervisor.

Other prohibited activity. In addition to the above, the following are prohibited uses of OPA computer systems, which is not intended to be exhaustive:

- Conducting illegal activities.
- Engaging in political activities.
- Accessing, downloading or uploading any material containing nudity or pornographic material.
- Gambling, wagering, betting, or selling chances.
- Engaging in any activity for personal gain or profit.
- Revealing or publicizing proprietary or confidential information which is not authorized.
- Representing one's personal opinion as the opinion of the OPA.
- Making or posting improper remarks and/or proposals (include but not limited to remarks that are defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually-oriented, threatening, racially offensive, or discriminatory statements, or illegal material).
- Uploading or downloading commercial software, music, movies, or other creative materials that violate copyright law.
- Participating in unauthorized "chat" rooms.
- Participating in unauthorized social networking sites, e.g., Facebook, MySpace, Twitter.
- Accessing sites outside the scope of normal job duties.
- Engaging in religious activities.
- Viewing sexually explicit material or pictures of nude adults or children.
- Making any personal unauthorized purchases or sales.

OPA staff must obtain approval from the Public Auditor for other uses of OPA computer systems for official work.

When in doubt, consult with your supervisor for clarification.

V. Discipline.

Violation of this policy may result in limiting or revoking access to OPA computer systems, Internet access, email use, etc. in addition to other disciplinary action determined to be appropriate by management. If your job duties require access to OPA computer systems and you are restricted from access to these job related tools, you will be impairing your ability to do your job and possibly impacting future job evaluations.

Violation of this policy may result in employee disciplinary action up to and including termination from employment.

Where guidance or interpretation of this policy is needed concerning the appropriateness of a particular use, you are advised to discuss the situation with your supervisor seeking further guidance and direction as necessary.

VI. Internet Access.

OPA computer systems that access the Internet are limited to OPA work-related purposes only. OPA staff use of OPA computer systems must be consistent with performing OPA duties.

The Internet can be a strong business tool. It provides access to information quickly, provides opportunities for everyone to access OPA reports, and provides the means to communicate instantaneously.

The Internet can also be a threat because it provides the opportunity for surreptitious access to OPA computer systems. Internet connections allow computer viruses or other malicious, incompatible or damaging programs into the OPA computer systems. A computer virus is most often introduced into a computer and interconnected systems through downloading of programs, documents, pictures, music or other data via the Internet.

VII. E-Mail

E-mail is a convenient and efficient communication tool. By recognizing that e-mail messages are very likely public records, the management, maintenance, retention, and proper disposition of these records can reduce the risks of litigation and loss of important information.

E-mail shall be used for business matters directly related to OPA activities.

E-mail shall not be used for personal gain, outside business activity, political activity, religious activity, fundraising, or charitable activity not sponsored by the OPA.

E-mail shall not be used to promote discrimination on the basis of basis of age, disability, gender, race, religion, national origin, sexual preference, or any other classification protected by law.

Personal use of e-mail must not interfere with normal OPA activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not be potentially embarrassing.

All e-mail messages sent or received on OPA computer systems are public records and may be subject to The Records Management Act and the Sunshine Reform Act of 1999.

The OPA reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose. Supervisors may review staff e-mails to determine security breaches, policy violations, or unauthorized actions.

VIII. Social Media

OPA's social media policy applies to both work and personal purposes, whether in normal work time or not, and on OPA computer systems or personal devices. OPA staff are prohibited from using OPA computer systems for social media (e.g., Twitter, YouTube, Facebook, etc). The OPA does not have a social networking account and does not engage in social networking sites. However, staff, on occasion may generally engage in incidental personal use of social media during permitted breaks on personal devices as long as such use does not interfere with operations and productivity, or violate OPA policies.

Responsible Use of Social Media. OPA does not have direct control over staff disclosures on social networking sites. However, staff must remember to protect the OPA reputation, their own privacy and privacy of other staff, and the confidentiality of OPA information when posting to these sites. At a practical level, staff are advised to avoid posting anything they would not wish other colleagues (both internal and external) to see.

Any information OPA staff disclose through personal social networking accounts is in the staff's personal capacity and never on behalf of the OPA. If staff disclose their association with the OPA through social media for personal purposes, their published views should be presented as purely personal views and not representative of the OPA.

Confidential Information. OPA staff must not disclose confidential information or sensitive OPA related information through social media. It is OPA's policy to protect all working papers and documents. Such disclosure may breach Title 1 Guam Code Annotated Section 1909.1 Confidentiality of Investigations and violations may lead to disciplinary action and may be punishable as a felony of the third degree.

IX. Resignation of Staff.

When staff resign from the OPA, the responsible supervisor must properly retain and store public records contained on the former staff's OPA computer, including e-mail records. The former staff's access to OPA computer systems shall be revoked and access codes or personal password codes will be changed.

Prepared by:

YHechanova 12/1/15

Yuka Hechanova
Deputy Public Auditor

Approved by:

DFBrooks 12/15/15

Doris Flores Brooks, CPA, CGFM
Public Auditor