1. Purpose

To outline acceptable use and clarify the protection of State of Alaska (SOA) information assets and technology resources. Unacceptable use exposes SOA to unwarranted risk (e.g., virus attacks, compromised network systems, services and legal issues associated with data tampering, data theft and privacy).

2. Statutory Authority

Alaska Statute 44.21 designates the Commissioner of the Department of Administration (DOA) with the responsibility for oversight of all SOA executive branch information technology, fulfilling the role of the Chief Information Officer (CIO) for the State. The roles and responsibilities for statewide information security have been delegated to the Chief Security Officer (CSO) through the Enterprise Technology Services (ETS) division director, by the CIO.

Records owned by the Departments are subject to oversight as designated by the Commissioner of the department under AS 44.17. Record retention requirements are subject to State archivist statutes under AS 40.21.

3. Policy Scope

This policy is applicable to all SOA branches, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Acceptable Use.

5.1. Acceptable Use

5.1.1 Access for Authorized Purposes

Acceptable use applies to all personnel (e.g., employees, partners, contractors, consultants, temporaries, other SOA workers and workers affiliated with third parties or anyone having access to SOA information that is not directly accessible to the general public from a non-SOA network (e.g., Internet)) and the use of all information processing equipment, including but not limited to computer equipment, software, operating system, storage media, and network accounts providing electronic mail, World Wide Web (www) browsing, file transfer protocol (FTP), Windows © mobile devices, Smartphones, personal digital assistants (PDAs), etc. and further applies to resources owned, leased, or managed by SOA or its designees and to non-SOA resources used at SOA facilities in the conduct of SOA business.

Personnel must use SOA networks and associated systems for authorized business purposes only. Personnel must not access information, programs, or systems when such access is not required for an authorized business purpose. This includes system

administrators who must have system access rights due to their job responsibilities. Administrators must not view or otherwise access SOA user information without the express consent of the user, Executive Management or the Division of Personnel and Labor Relations (DOPLR).

SSO personnel will monitor equipment, systems, and network traffic at any time, for the purpose of security and network maintenance.

5.1.2 Personal Computing Equipment Prohibited Use

Personnel must not use personal computing equipment (e.g., laptops, PC, workstations, servers, external hard drive, USB devices, Smartphone or other networking equipment) within the SOA wide area network (WAN) or local area networks (LANs) for SOA or personal business. Personnel who connect a personal device to an SOA network or device in violation of this policy are exposing the device and all information on the device to potential monitoring, collection and public disclosure.

5.1.3 Contractors Computing Equipment Authorization

Contractors may use their personal or company owned devices within the SOA WAN or LANs, but these devices must be subject to all SOA policies when connecting to the SOA networks and will be monitored, reported and audited for security proposes. Contractors forfeit any right to privacy.

Contractors who connect personal or company owned devices to the SOA network acknowledge that all materials and information on each device are subject to monitoring, review, collection and public disclosure by State or federal statute, regulations, administrative order, policy or directive.

5.1.4 Application of Passwords

Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed regularly. Personnel must use passwords of strength, specific criteria and control to access and protect the SOA WAN and LANs and must adhere to what is defined in SOA policy ISP-178 Password Management.

With the exception of public-access terminals or by SOA SSO written authorization, all non-mainframe computers (e.g., servers, workstations, terminals and laptop computers) must be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less. When personnel leave a computer unattended this password-protected screensaver feature must be manually activated or the computer must be turned off.

5.1.5 Posting of SOA Sponsored Accounts

SOA sponsored accounts to news groups or web forums shall contain a disclaimer which states the opinions expressed are strictly the poster's own and not necessarily those of the SOA, unless posting is in the course of business duties.

5.1.6 Use of Issued Credentials

Personnel must use only the user IDs, network addresses, and network connections defined by the SOA or department information technology administration staff to access SOA networks and associated systems.

5.1.7 Unauthorized Security Tools

Personnel must not download, install, or execute any security program or utility (e.g., password cracker, network sniffer, vulnerability scanner) designed to reveal weaknesses in the security of a system without explicit authorization from the State Security Office (SSO).

5.1.8 Execution of Electronic Information

Personnel must use extreme caution when opening files that have been sent to or received either electronically or on removable media (e.g., floppy disk, CD/DVD, USB Flash drive). Examples of such files are email attachments received from unknown senders, files downloaded from the www or FTP sites, seemingly innocuous commercial files, etc. Any and all of these items can contain viruses, e-mail bombs, trojan-horse code, spyware/ad-ware, BOT net, other malware, or inappropriate material and should be suspected. If personnel experience unusual computer symptoms when opening unknown files, they must report these to their department IT staff immediately. If contractors with SOA business suspect any of the above listed items they shall disconnect from SOA network and notify their client supervisor immediately for remediation in all efforts to protect SOA information assets.

5.1.9 Unacceptable Use

Under no circumstances are personnel of the SOA authorized to engage in any activity that is illegal or in violation of local, State, federal or international law, or Alaska Administrative Code.

Prohibited email, communication activities, system and network activities are listed below. Personnel may be exempted from some of these restrictions during the course of their valid job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services or the requirement of a law enforcement investigation) however, cautious and meticulous adherence must be followed by all users.

5.1.9.1 E-mail and Communications Prohibited Activities:

- Any illegal activity.
- Intentionally sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
- Any form of harassment via email, instant messaging, telephone, paging, or other electronic means, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within SOA networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SOA or connected via the State's network.
- Posting the same or similar non-business-related messages to Usenet news groups or web forums.
- Use for access to or distribution of indecent or obscene material, including child pornography.
- Use for commercial activities, including advertising, unless specific to charter, mission, or duties of the government agency.

- Use for fundraising, political campaign or partisan activities, or public relations activities not specifically related to SOA government activities.
- Use of SOA information technology resources for personal gain.

5.1.9.2 System and Network Prohibited Activities:

- Violations of the rights of any person or company protected by copyright "©", or trade mark "™" or registered "®", or trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the SOA.
- Unauthorized copying of Copyright Material "©" including, but not limited to, digitization and distribution of photographs from magazines, books or other copyright sources, copyright music, and the installation of any copyright software for which the SOA or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Intentional introduction of malicious programs into SOA information technology resources (e.g., introducing viruses, worms, Trojan horses, e-mail bombs, etc. into the SOA network or individual SOA computing devices).
- Revealing account information to others or allowing use of a personal account by others. This includes family and other household members when work is being done at home.
- Using SOA computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any SOA account.
- Intentionally causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forging route information for malicious purposes.
- Network vulnerability testing, security scanning, virus or Trojan horse testing or executing any form of network monitoring, which will intercept data not intended for the user's host.
- Any activity, application or service that disables, tampers with, circumvents security solutions, services, controls, user authentication, security of any host, network or account, or interfering with or denying service to any authorized user or service is prohibited and strictly enforced. (e.g., URL filtering, network monitoring, remote access requirements through SOA virtual private network, SOA ingress/egress access control requirements, Cisco Security Agent, and other security solution, service, or control, intentionally evading a security solution or process, or creating a denial of service to a user, applications, host, network, or other SOA process).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable another user's terminal session via any means, locally or via the Internet/intranet/extranet.
- Providing information about or lists of SOA personnel to any outside parties, without a business case or SSO approval.

- Personal use of or divulging of private or confidential information regarding any individual obtained by any personnel, as a result of performance of job duties or as a result of their employment with the SOA.
- Use of encryption (at rest or in transit) without an approved business case justification and written approval from the ISO Designee and the SSO.
- Uses of peer-to-peer (P2P) file transfer solutions (e.g., Gnutella, BitTorrent, etc.) without an approved business case justification and written approval from the Department Information Security Officer (ISO) and the SSO.
- Use of non-standard, non-SOA provided instant messaging technologies (e.g., Skype, MSN, AOL, Googletalk, etc.) or other similar technologies without an approved business case justification and written approval from the Department Information Security Officer (ISO) and the SSO.
- Use of non-standard remote control technologies (e.g., GoToMyPC, Dameware, Radmin, etc.) or other similar technologies.
- Use of non-operating system standard screen saver or other similar technologies.
- Use of any external proxy systems or other similar technologies.
- Use of any program or application that performs off-site document or file indexing (e.g., Google Desktop) or other similar technologies.
- Use of any streaming media technologies (e.g., Radio, YouTube, etc.) without an approved business case justification and written approval from the Department Information Security Officer (ISO) and the SSO.

5.1.10 Least Privilege

Personnel tasked with network user administration must ensure that network and system access controls are configured to limit the privileges extended to users to the least necessary to accomplish authorized business purposes.

5.1.11 Applicable Statutes and Enforcement

The Executive Branch Ethics Act states a public employee may not "**use state time, property, equipment, or other facilities to benefit personal or financial interests**" (AS 39.52.120(b)(3)). Further, "standards of ethical conduct for members of the executive branch need to distinguish between those minor and inconsequential conflicts ... and those conflicts of interests that are substantial and material." (AS 39.52.110(a)(3)).

The Executive Management acknowledges that incidental personal use may be unavoidable in today's electronic environment. In cases where SOA office technology incidental personal use occurs, users must be aware that there is no right to privacy regarding these occurrences. Applicable Statutes, Administrative Orders and Codes include, but are not limited to: AS 39.52, Alaska Executive Branch Ethics Act; Administrative Order #81, Nondiscrimination and Non-Harassment; Administrative Code 9 AAC 52, Alaska Executive Branch Code of Ethics; AS 39.25.160, Alaska Little Hatch Act; AS 24.60, Legislature Standards of Conduct.

Personnel found to have violated this policy are subject to discipline up to and including dismissal.