State of Alaska
Office of Information Technology
Information Security Policies

Title:	Third Party Security	Effective:	7/1/2017
Number:	ISP-112	Last Review:	7/1/2017
Version:	1.01	Next Review:	Annually
Pages	3	Approved by:	CIO
		Distribution:	SOA

1. Purpose

To define the information security expectations of the State of Alaska (SOA) when conducting business with vendors, contractors, business partners, and other third party entities with authorized access to SOA information and information assets operating within or on behalf of the SOA.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

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 requirements for:

- Risk management;
- Third party access;
- Third party agreement; and
- Third party management.

5.1. Risk Management

5.1.1 Risk Assessment and Third Parties

Executive Management must ensure that risks related to a third party accessing, processing, communicating, or managing SOA information or information processing facilities are identified and appropriately addressed.

5.2. Third Party Access

5.2.1 Security of Information

Executive Management must ensure that the information security requirements of SOA information systems are identified, and that appropriate controls are implemented to safeguard such information systems, prior to granting access to third parties.

5.3. Third Party Agreements

5.3.1 Security Requirements in Third Party Agreements

Executive Management must ensure that an agreement covering relevant security requirements is in place for any third parties providing services involving accessing, processing, communicating, or managing SOA information or information processing facilities. Such an agreement must include non-disclosure definition, ownership of information, systems and services, confidentiality requirements, information retention and/or destruction during and post-mortem of agreement, service definitions, delivery levels, service management aspects, or other applicable security controls expected of the third party, or of the SOA, as appropriate to the service, agreement or contract.

5.3.2 Monitoring Compliance with Third Party Agreements

Executive Management must ensure that services of third parties are monitored to verify compliance with the security requirements of agreements. Such monitoring must include review of reports or records generated regarding the service or other criteria appropriate to the service.

Executive Management must ensure appropriate performance audits are conducted to respond to information security incidents or in accordance with the terms of service agreements. The State Security Office (SSO) or the Department of Law must provide guidance to Executive Management, as necessary, in support of issues of security or contract compliance and enforcement.

5.3.3 Updating Third Party Agreements

Executive Management must periodically review changes to the organization, its policies, and its systems to identify changes to the security requirements of third parties. When security requirements change, Executive Management must determine, whether modification of third party agreements is necessary and, if needed, must coordinate with internal or external counsel and DOA Division of General Services as well as with the applicable third parties to address the proposed changes to agreements.

Executive Management must immediately notify the DOA Division of General Services and the SSO of any material change in the SOA relationship with a third party service provider, including but not limited to:

- enhancements to the services offered;
- development of new applications and systems;
- modifications to SOA policies and procedures;
- termination of services; and
- loss of personal or sensitive information.

5.3.4 Maintenance of Third Party Agreements

Executive Management and/or internal counsel must maintain an original copy of each executed third party agreement in accordance with SOA record retention policies.

5.3.5 Exchange Agreements

Executive Management must establish agreements for the exchange of information and/or software between the SOA and external parties. These agreements must include assurances for the security of SOA information throughout the agreement's life cycle and the return or certified disposal of SOA information upon termination of agreements.

5.4. Third Party Management

5.4.1 Changes to Third Party Services

Executive Management must manage changes to services, products, processes, procedures, or controls that impact the security and information assets of the SOA and ensure changes are accurately documented and communicated to DOA Division of General Services.