		Effective:	7/1/2020
		Last Review:	7/1/2020
Title:	Cloud and Offsite Hosting	Next Review:	Annually
Number:	ISP-196		
Version:	1.01	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

The State of Alaska (SOA) must establish information security requirements for procuring and utilizing cloud or offsite hosting services.

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). This policy applies to all Information Technology (IT) related RFPs, contracts or service agreements initiated after the effective date. This policy does not preclude use of Software as a Service (SaaS) solutions which include integrated cloud elements that are solely used by and are specific to that solution.

4. Definitions

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

5. Policy Statement

This policy stipulates:

- Cloud and Offsite Hosting.

5.1 Cloud and Offsite Hosting

5.1.1 Cloud Smart Strategy

The State of Alaska has a cloud smart strategy which balances aggressive cloud adoption with business value assessment. New and renewed services should look for cloud services before in-house solutions based on cost and efficiency.

5.1.2 Mandatory Terms and Conditions

Every Cloud computing engagement must include the Mandatory Terms and Conditions clauses (see SOA Cloud Computing Standards) and a cloud exit assessment/strategy/ plan.

5.1.3 Formal Authorization

Use of cloud computing services for work purposes must be formally authorized by the Department of Administration (DOA) Chief Information Officer (CIO), the Department of Administration (DOA) Chief Information Security Officer (CISO), and agency/department Admin Services Director (ASD) through the approved Statewide IT governance model.

5.1.4 Platform Certification

The State Security Office (SSO) will certify that security, privacy and all other IT management and security requirements will be adequately addressed by the cloud computing vendor and that they conform to SOA Cloud Computing Standards.

5.1.5 Compliance

The use of such services must comply with SOA's policies, standards and procedures, data sovereignty requirements, laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by the SOA and shall be audited for compliance annually or as needed by the SOA signatory.

5.1.6 Credential Vault

The SSO department will keep a confidential and secure repository containing account information for business continuity purposes.

5.1.7 Personal Accounts Prohibited

Personal cloud services accounts may not be used for the storage, manipulation or exchange of SOA-related communications or SOA-owned data.

5.1.8 FedRAMP Preference

The Office of Information Technology (OIT) recommends the use of Federal Risk and Authorization Management Program (FedRAMP) listed/compliant cloud computing vendors. Non-FedRAMP listed/compliant cloud computing vendors may only be used after review and approval by the appropriate Statewide IT governance body.

5.1.9 Single Sign-On with SOA Federation

Cloud services that integrate with employee's existing network credentials reduce the number of passwords employees need to maintain and promote efficiency and security.